Vysoká škola logistiky o.p.s.

Technologie Blockchain v logistice

(Bakalářská práce)

Přerov 2021 Jason Parker Kubik, DiS.

Vysoká škola logistiky o.p.s.

Zadání bakalářské práce

student	**Jason Parker Kubik, DiS.**
studijní program	LOGISTIKA
specializace	Informatika pro logistiku

Vedoucí Katedry bakalářského studia Vám ve smyslu čl. 22 Studijního a zkušebního řádu Vysoké školy logistiky o.p.s. pro studium v bakalářském studijním programu určuje tuto bakalářskou práci:

Název tématu: **Využití technologie Blockchain v logistice**

Cíl práce:

Navrhnout možnosti využití technologie Blockchain v oblasti logistiky. Návrhy demonstrovat na typových příkladech.

Zásady pro vypracování:

Využijte teoretických východisek oboru logistika. Čerpejte z literatury doporučené vedoucím práce a při zpracování práce postupujte v souladu s pokyny VŠLG a doporučeními vedoucího práce. Části práce využívající neveřejné informace uveďte v samostatné příloze.

Bakalářskou práci zpracujte v těchto bodech:

Úvod
1. Popis technologie Blockchain
2. Služby a aplikační možnosti technologie Blockchain v současné informační logistice
3. Návrh systémového využití platformy EIA Blockchain v oblasti průmyslových transakcí
4. Vyhodnocení vlastního návrhu a možnosti aplikačního nasazaní EIA Blockchain

Závěr

Rozsah práce: 35 – 50 normostran textu

Seznam odborné literatury:

ELA Blockchain services [online]. Praha: Elektrotechnické asociace České republiky, 2019 [cit. 2019-10-30]. Dostupné z: https://www.elachain.cz

JAŠEK, Roman, Martin BURDÍK a Michal SEDLÁČEK. Blockchain v logistice. In: LOGISTIKA -EKONOMIKA - PRAX 2018: Mimoriadne číslo internetového portálu Logistický monitor - http://www.logistickymonitor.sk/images/prispevky/zborniklep-2018.pdf. Žilina: Logistický monitor, 2018, s. 61-68. ISSN 1336-5851.

LEE, David a Robert DENG, ed. Handbook of blockchain, digital finance, and inclusion. London: Academic Press, [2018]. ISBN 978-0-12-812282-2.

SOMMERVILLE, Ian. Softwarové inženýrství. Brno: Computer Press, 2013, 680 s. ISBN 9788025138267.

Vedoucí bakalářské práce:	prof. Mgr. Roman Jašek, Ph.D.
Datum zadání bakalářské práce:	31. 10. 2020
Datum odevzdání bakalářské práce:	6. 5. 2021

Přerov 31. 10. 2020

Ing. et Ing. Iveta Dočkalíková, Ph.D.
vedoucí katedry

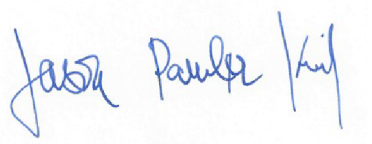
prof. Ing. Václav Cempírek, Ph.D.
rektor

Čestné prohlášení

Prohlašuji, že předložená bakalářská práce je původní a že jsem ji vypracoval samostatně. Prohlašuji, že citace použitých pramenů je úplná a že jsem v práci neporušil autorská práva ve smyslu zákona č. 121/2000 Sb., o autorském právu, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

Prohlašuji, že jsem byl také seznámen s tím, že se na mou bakalářskou práci plně vztahuje zákon č. 121/2000 Sb., o právu autorském, právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména § 60 – školní dílo. Beru na vědomí, že Vysoká škola logistiky o.p.s. nezasahuje do mých autorských práv užitím mé bakalářské práce pro pedagogické, vědecké a prezentační účely školy. Užiji-li svou bakalářskou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědom povinnosti informovat o této skutečnosti Vysokou školu logistiky o.p.s.

Prohlašuji, že jsem byl poučen o tom, že bakalářská práce je veřejná ve smyslu zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, zejména § 47b. Taktéž dávám souhlas Vysoké škole logistiky o.p.s. ke zpřístupnění mnou zpracované bakalářské práce v její tištěné i elektronické verzi. Tímto prohlášením souhlasím s případným použitím této práce Vysokou školou logistiky o.p.s. pro pedagogické, vědecké a prezentační účely.



V Přerově, dne 13. 08. 2021 .....

podpis

Poděkování

Děkuji tímto vedoucímu práce prof. Mgr. Romanu Jaškovi, Ph.D., DBA za jeho odborné vedení a cenné rady, které mi pomohly rozšířit vědomosti v oblasti technologie blockchain a pochopení významu použití v logistice a dalších odvětvích.

Anotace

Bakalářská práce je zaměřena na využití technologie blockchain ve farmaceutickém průmyslu s ohledem na její logistické procesy při výrobě a distribuci vakcín a ověřování výrobních a logistických procesů formou využití ElA Blockchainu. V teoretické části je popsáno fungování blockchainu z pohledu bezpečnosti, architektury, využití frameworků, ale také jeho vývojové etapy a využití v logistice a dalších odvětvích. Praktická část představuje návrh využití blockchainu a ElA Blockchainu ve farmaceutickém průmyslu. Tato práce také vyhodnocuje přínosy návrhu pro konkrétní odvětví.

Klíčová slova

Blockchain, hash, IT bezpečnost, farmaceutický průmysl, ElA Blockchain, Blockchain Notarius

Annotation

The bachelor thesis focuses on using of blockchain technology in the pharmaceutical industry concerning its logistics processes in the production and distribution of vaccines and its verification. All this is possible thanks to ElA Blockchain. The theoretical part describes the functioning of the blockchain in terms of security, architecture, use of frameworks, and its development stages and used in logistics and other industries. The practical part presents a proposal for implementing blockchain and ElA Blockchain in the pharmaceutical industry. This thesis also evaluates the benefits of the proposal for specific sectors.

Keywords

Blockchain, hash, IT Security, pharmaceutical industry, IEA Blockchain, Blockchain Notarius

Obsah

Úvod

Tato bakalářská práce se zaměřuje na vysvětlení a poskytnutí komplexních informací o fungování technologie blockchain a jejího uplatnění v logistických procesech. Zjednodušeně, jedná se o určitý typ decentralizované databáze, která je spravována pouze zapojenými uživateli v konkrétně zřízené blockchainové síti, čímž je vyřešena i stránka její bezpečnosti. Blockchain je velice skloňovaný termín vzhledem k faktu jeho neomezeného využití napříč odvětvími při nakládání s daty. V první kapitole jsou zmíněny informace o vzniku a historii blockchainu, jeho jednotlivé vývojové etapy, typy sítí, typy frameworků a konsenzuální mechanismy. Kapitola by sama o sobě měla poskytnout základní přehled o technologii. Druhá kapitola pojednává o bezpečnosti tohoto řešení, neboť se jedná o jednu z primárních myšlenek blockchainu, která následně navazuje na třetí kapitolu představující logiku architektury. Poslední část teorie se zaměřuje na uplatnění v klíčových oborech, jakými jsou logistika, průmysl a dodavatelský řetězec.

Cílem bakalářské práce je vyhotovení vlastního návrhu využití platformy ElA Blockchain v průmyslových transakcích, konkrétně ve farmacii. Projekt ElA Blockchain je v současné chvíli určen pro české právnické subjekty. Praktická část je rozdělena na dvě řešení. V první části je navrženo řešení sledováním inkrementovaných údajů při výrobě očkovacích látek a sdílením v permissioned blockchain síti s konkrétními zdravotnickými zařízeními očkujícími vakcínou proti SARS-COVID-2019.

V druhé části je popsáno, jak využít tuto platformu ve farmaceutickém průmyslu na globální úrovni. Představena je také jedna ze základních aplikací Blockchain Notarius, která je klíčovým prvkem a základním stavebním kamenem projektu ElA Blockchain pro navrhované řešení. V práci je uvedeno, jak využít platformu pro ověření pravosti dokumentace výrobních a logistických procesů při výrobě vakcín sdílených s jednotlivými očkovacími centry a dohledovými orgány v jednotlivých státech.

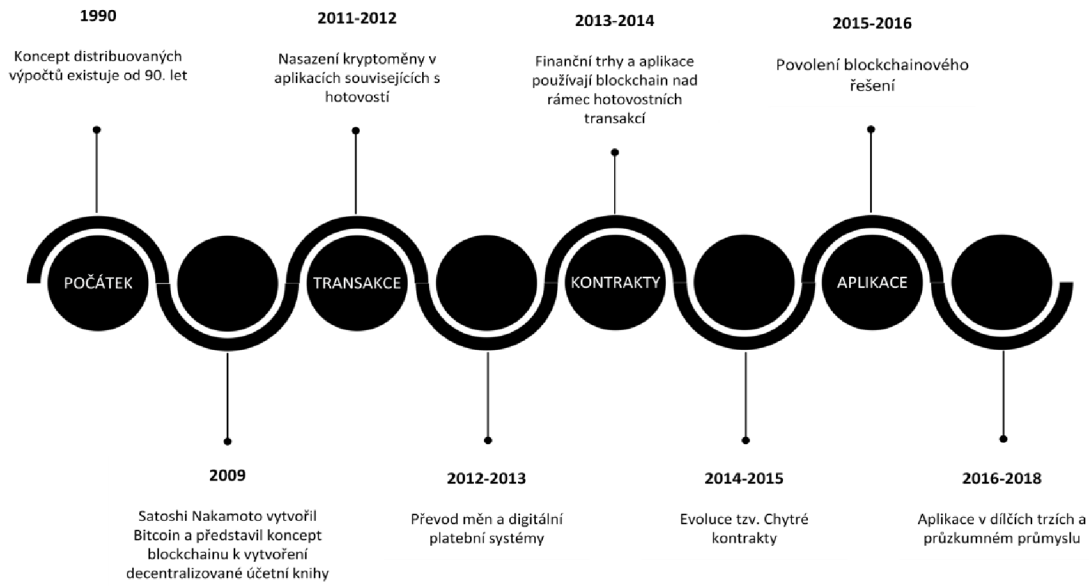
Navrhované řešení může posloužit jako primární myšlenka pro realizaci řešení ve farmaceutickém průmyslu a může být dále podrobena detailnějšímu rozpracování. Z hlediska jeho absence je řešení více než vhodné pro dané odvětví, jehož přínosy jsou shrnuty ve vyhodnocení návrhu práce.

1 Blockchain

Technologie, která přinesla převrat v oblasti decentralizované správy za současného držení vysokých bezpečnostních standardů, a zároveň umožnila své využití napříč odvětvími. Blockchain není jen soustředění různých transakcí a informací do bloků a řetězců, jak název napovídá. Je to fungující a promyšlená systémová logika vycházející z historické potřeby vytvořit systém přístupný všem, avšak se silným důrazem na integritu dat. Blockchain je provozován prostřednictvím distribuované sítě účastníků, kteří si navzájem nemusí nutně důvěřovat, avšak dodržují stejná pravidla shody [1].

1.1 Vznik

Původní myšlenku technologie blockchain a její využití v praxi bychom mohli datovat v předcházející dekádě, konkrétně v roce 2008. Tehdy Satoshi Nakamoto publikoval krátkou rešerši Bitcoin: A Peer to Peer Electronic Cash System. Primárně se jednalo o její popis a fungování, nicméně bez blockchainu by toto nebylo možné. Další součástí je i nastínění a představení technologie jako nové systémové služby. Ve velice krátkém čase se začala kryptoměna používat jako platební instrument, a na tomto základě začaly vznikat další elektronické měny.



Obr. 1.1 Historie vývoje blockchainu

Zdroj: vlastní zpracování.

Příchodem dalších způsobů jejího aplikování se začalo uvažovat o využití blockchainu jinak než jen pro transakce kryptoměn. Tím hlavním hybatelem bylo Ethereum, které uvolnilo open-source označovaný jako „smart kontrakty“, jenž umožňovaly vytvářet vlastní skripty. V současné chvíli jsou tyto kontrakty nedílnou součástí každého blockchainu, který se zavádí.

1.2 Vývojová etapy

1.2.1 Blockchain 1.0

Jedná se o úplně první generaci blockchainu, který vznikl za účelem realizace platebních transakcí vytvořením uceleného systému s elektronickou měnou (bitcoin), jenž by nebyl řízen ústřední autoritou, ale zároveň byl bezpečný, neměnný a decentralizovaný.

Tato generace je postavena na 3 prvcích:

- blockchain – uchovává transakce v blocích,
- token – je chápán jako zůstatek uživatele či identifikátor transakce,
- protokol – logika systému (např. různá pravidla pro ověřování bloku).

1.2.2 Blockchain 2.0

Zásadní změnou oproti předchozí verzi je možnost využití smart kontraktů. Tyto kontrakty jsou chápány jako programovací kódy s vlastními identifikátory, funkcemi a proměnnými. Proto mají takové uplatnění v blockchainu jako takovém. Jejich nezaměnitelnost jim dává unikátní identifikaci, a proto se využívají pro transakce v blockchainu. Tyto transakce mohou být realizovány skrze smart kontrakty, které uvolňují předem nadimenzované funkce prostřednictvím aplikace.

Při hlubším pochopení smart kontraktu jde o převratnou logiku, která dokáže sama na základě své legitimity řídit operace z něj vycházející a zajistit tak vypořádání této virtuální měny mezi dvěma subjekty. Typickým příkladem této generace je již dříve zmíněné Ethereum, které jim položilo základ, a tak se staly součástí blockchainu.

1.2.3 Blockchain 3.0

Jde o aktuální verzi, která je především v duchu inovací verzí předcházejících, zdokonalující nedostatky, které si s sebou nesly. Jedním z nejznámějších úskalí byla škálovatelnost. Kromě nízké propustnosti transakcí u blockchainu, které využívají konsensus Proof-of-Work, narážejí na problémy pomalého zpracování a užití velkého množství výpočetního výkonu a energie. Řešením byl protokol Proof-of-Stake, který pracuje s tzv. epochami. Ty chápeme jako určitý časový úsek, jenž dělíme na menší celky neboli sloty.

1.3 Princip

1.3.1 Rozdělování výpočetního výkonu

Výpočetní síla konkrétní blochckain sítě je rozdělena mezi všechny její uzly, které jsou do ní zapojeny. Podstata fungování takové sítě je na principu peer-to-peer. Spojení myšlenky blockchainu a konceptu peer-to-peer sítě má svá velká pozitiva, co se týče stability sítě a hodnoty její výpočetní síly. V situaci, kdy máte několik tisíc uzlů, výpadek jednoho uzlu nebo malé skupiny uzlů nemůže ovlivnit provoz sítě, či dokonce její vypnutí. Za jistý provozní incident bychom mohli však považovat situace, kdy se více jak polovina těchto uživatelů pokusí přemoci menší skupinu uživatelů. Ovšem takový typ v podstatě řízeného kybernetického útoku nebude anonymní a všichni si budou vědomi toho, co se právě odehrává. Můžeme s přesvědčením říci, že taková situace je v podstatě nereálná. Výpočetní výkon je tedy principiálně nenapadnutelný.

Zároveň je blockchain chráněn proti jiným vstupům, jakými mohou být vládní agentury, stát, či korporace. Když vezmeme v úvahu konsenzuální algoritmus Proof-of-Work, jakožto jeden ze známých algoritmů aplikovaných v síti blockchain, útočník by potřeboval enormně vysoký vlastní výpočetní výkon. V takovém případě by pro útočníka pozbyl útok na atraktivitě, neboť principem je získat data a další informační aktiva za přijatelnou cenu, které pak může zhodnotit. Zde by náklady převyšovaly jeho motivaci.

1.3.2 Síťová integrita

Integrita je stav, kdy dojde k souladu mezi dvěma stranami na činnostech, které byly sjednány. Může tedy jít o přijetí rozhodnutí a stanovení postupu při nenadálé události.

V síti blockchain však toto není závislé pouze na jednom uzlu či instituci, avšak je to souhrnně vyžadováno blockchain sítí, aby ona samotná, a tedy všichni její účastníci, dodržovali její integritu.

I přesto, že integrita je předem dána, tedy implementována do jednotlivých kroků všech procesů a její mechanismy není lehké obejít, správným chováním přispívají jednotlivci k jejímu povědomí. Porušení těchto mechanismů je pro útočníka nevýhodné stejně tak, jako pokus o převzetí, či sabotáž výpočetního výkonu blockchain sítě.

1.3.3 Bezpečnost

Výhodou blockchainu je skutečnost neexistence bodu selhání, a to díky skutečnosti, kdy veškeré prvky jsou součástí kódu sítě a každý, kdo chce být součástí konkrétní sítě blockchainu, musí přijmout používání kryptografie. I přes jistou anonymitu v blockchain síti zajišťují tyto prvky ve zdrojovém kódu důvěryhodnost.

V době, kdy různé instituce nakládají s daty různé povahy, ať už jde o data zdravotní, bankovní, osobní, a zároveň kdy na uživatele internetu číhá spousta nástrah, od používání nedůvěryhodných zdrojů, emailových phishingů, podvržení session, je potřeba věnovat bezpečnosti velice vysokou pozornost. Ne vždy se tomu tak děje. Dle společnosti IBM, která v roce 2020 provedla studii, je průměrná celková cena nákladů související s odcizením dat 3,86 miliónů amerických dolarů, přičemž průměrná cena odcizeného datového záznamu byla stanovena na 175 amerických dolarů. Tato skutečnost jen zesiluje fakt, že veškerá data mají svou cenu, kterou si společnosti neumí vždy stanovit. S ohledem na tuto skutečnost je proto lepší chovat se preventivně než následně korektivně, a považovat tak bezpečnost za klíčový faktor, který blockchain splňuje.

1.3.4 Soukromí

Soukromí zahrnující ochranu naší identity a dat patří v dnešní době mezi jednu z nejvíce ceněných komodit, můžeme-li to takto nazvat. Důvodem je rostoucí potřeba korporací zvyšovat jejich zisky. Proto investují nemalé finanční prostředky do analýzy dat, jejich zpracování a vytěžování. Na jedné straně zde máme korporace, které z povahy svého podnikání o poskytovaných službách klientům mají taková data chránit, na druhou stranu se snaží získat další osobní data a kontakty pro případnou akvizici a optimalizaci

obchodní strategie. Ať už tak či onak, zde opět vstupuje do hry blockchain a jeho benefity, které z něj vychází.

V blockchainu není potřeba znát jméno, datum narození či email k tomu, aby bylo možné jeho benefity využívat. Postačí nám mechanismy kryptografie a veřejné klíče. Avšak pokud tento veřejný klíč není nikde zaznamenán pro dohledání, jedná se stále o neidentifikovatelnou osobu z pohledu její identity, nicméně autorizovanou k provádění transakcí a dalších úkonů v síti.

1.3.5 Udržení práv

Tak, jak se doba posouvá k absolutní digitalizaci a mění se i potřeby společnosti, je čím dál více obtížné udržet krok s prokazováním pravosti různých děl. O to více těch, která nejsou digitalizovaná, či v digitálním světě nevznikla. Avšak budoucnost nám pomalu ukazuje směr, jak bychom mohli tuto tvorbu ověřovat. Již nyní existuje situace, kdy si koupíte nějaké dílo a dostanete k němu certifikát pravosti. Bohužel se zvyšující se digitalizací a pokrokem doby a technologií nestačí pouze PDF dokument prokazující vlastnictví originálu historického díla. Za pomoci databáze registrující všechna díla, moderní kryptografií a nezaměnitelností hashe se prokáže, že jste skutečným vlastníkem pravého obrazu či antické vázy, a toto bude také zpětně dohledatelné v databázi děl a blockchain síti. Zní to jako hudba budoucnosti, nikoliv však jako utopie. V následujících letech budeme prokazovat identitu a vlastnictví pomocí moderních technologií, kryptografie a blockchainu.

1.4 Typy sítí

1.4.1 Public

Jedná se o veřejně přístupný decentralizovaný systém, ke kterému má přístup každý, kdo disponuje internetovým připojením a „open-source“ systémem k tomuto účelu vymezeném. Ten, kdo splní tyto podmínky a stane se součástí blockchainu, může nahlížet prostřednictvím svého uzlu na zrealizované a současné transakce a podílet se na algoritmu uplatňovaného v síti blockchain, který je podstatou při zveřejňování jednotlivých bloků. Každý uzel je tedy oprávněn ke čtení, zápisu a zároveň auditu. Všichni jsou si zde rovni

bez dohledu centralizované autority a závislosti na jednom výpočetním výkonu, což není podmínka veřejné sítě, ale služby jako takové.

Pozitiva:

- Důvěra – primární algoritmus Proof-of-Work, na kterém blockchain jako takový vznikl, má velký benefit v principu provádění transakcí bez potřeby důvěry mezi uzly. K tomu všemu je veřejný blockchain navržen primárně tak, aby zde bylo minimalizováno zneužití.
- Bezpečnost – v blockchainu obecně platí, že čím větší síť je, tím je bezpečnější. Pro útočníka je s rostoucí velikostí útok více komplikovaný a z pohledu proveditelnosti cíleného útoku na konkrétní vektor téměř neproveditelný. Důvodem je prvně vysoký počet uzlů, a pak decentralizace systému z toho vycházející. Navíc, tento typ blockchainu není limitován počtem uživatelů.
- Transparentnost – vysoká úroveň transparentnosti je vlastně podstatou veřejného blockchainu, díky možnosti každého uzlu číst, zapisovat a provádět audit a dále možnosti sledovat jak historické, tak současné transakce.

Negativa:

- Rychlost – neomezený počet uzlů je na jedné straně výhodou, avšak může být i Achillovou patou systému. Pokud zde stojíme před principem zpřístupnit veřejný blockchain každému, a zároveň je zde princip decentralizace, je zcela zřejmé, že systém s konsenzuálním mechanismem Proof-of-Work nemůže být rychlý, neboť každá nová transakce před zveřejněním do bloku musí být validována každým uzlem. Aby se systém nezhroutil, je možné realizovat pouze nízký počet transakcí.
- Škálovatelnost – současně vysoký počet transakcí a odesílání bloku je velice náročné jak na čas, tak výpočetní výkon. Z tohoto důvodu jsou veřejné sítě znevýhodněné a škálovatelnost je zde v tomto případě velice neefektivní.

1.4.2 Private

Privátní blockchain nese trochu jiný smysl fungování. Základní myšlenka je založena na veřejném blockchainu, avšak je určena pouze pro určité uživatele. Jejich autorizace, oprávnění a zabezpečení této privátní sítě je v držení centrální autority. Účastník se může do takové soukromé sítě připojit pouze prostřednictvím autentické a ověřené pozvánky

[2]. Tento typ sítě je většinou součástí nějaké společnosti ve smyslu organizace. Z důvodu privátní sítě blockchainu lze říci, že se jedná o důvěryhodné prostředí, neboť centrální autorita určuje uživatele této sítě.

Pozitiva:

- Rychlost – z důvodu limitovaného počtu uživatelů (uzlů) je rozsah sítě podstatně menší, než tomu bývá u jeho veřejného typu. Dalším benefitem je důvěra mezi uzly v privátní síti. Díky ní je možné používat i jiné typy konsenzuálních algoritmů, a tedy lze rychleji dosáhnout shody. Oproti veřejnému blockchainu může rozdíl v rychlosti zpracování transakcí šplhat až do tisíců za sekundu.
- Škálovatelnost – vzhledem k mnohonásobně menšímu počtu uzlů oproti veřejnému blockchainu se zvyšuje také exponenciálně jeho škálovatelnost.

Negativa:

- Centralizace – způsobila vzdálení se od původní myšlenky sítě blockchain, kde bylo podstatou mít sdílený výpočetní výkon a být čistě decentralizovaný s možností provádět transakce i mezi neověřenými uzly. Vzhledem k tomu, že v privátním blockchainu je každý uzel identifikován před přidělením práv a přidáním do sítě, je zde potřeba administrátora, který má toto na starost. Dochází tedy k ověření identity a jejich správě. Vývoj a využití této technologie napříč odvětvími v soukromém sektoru a korporacích není vždy decentralizace a absolutní transparentnost žádoucí.
- Bezpečnost – jelikož je síť centralizovaná a má mnohonásobně méně uživatelů, je v takovém případě i snazším cílem pro útočníky.

1.4.3 Permissioned

Permission blockchain umožňuje propojení veřejných a soukromých blockchain sítí za podpory mnoha možností přizpůsobení [2], kde si může sama instituce rozhodovat o různých právech pro čtení a různých právech pro realizaci transakcí u konkrétního uživatele či konkrétní skupiny uživatelů. Tento typ sítě může a nemusí být otevřený pro všechny. Jelikož se jedná o síť s mnoha možnosti proměnných v jejím nastavení, je vymezena samostatně jako další možnost typu sítě. S permissioned blockchain se můžeme často setkat v komerčním využití, kde se jeví jako velice užitečná.

Pro modelaci je možné uvést spotřebitelsko-dodavatelský trh potravin. Obchodní řetězce se dnes často setkávají s potřebou zákazníků znát původ masa, jakým způsobem chovu prošlo a jakým procesem prošlo během svého života od chovu, přes porážku až na chladící pult v konkrétním obchodním domě v rámci jeho distribuční sítě. Východiskem této modelové situace je skutečnost, že všechny tyto informace budou poskytovat chovatelé dobytka všem svým odběratelům, které představují jednotlivé obchodní řetězce. Tyto informace by pak jednotlivé obchodní řetězce poskytly zákazníkům k ověření prostřednictvím front-end aplikace. Samozřejmě všechny informace, které chovatelé sdílí s obchodními řetězci, nemusí a nesmějí být poskytnuty koncovému spotřebiteli, jako jsou nákupní ceny a jiné citlivé obchodní informace. Z tohoto důvodu si chovatelé mohou stanovit, které informace budou určeny všeobecně pro koncového spotřebitele, tedy tak i pro všechny obchodní řetězce, dále informace, které budou určené výhradně obchodním řetězcům až na úroveň cen pro jednotlivé obchodní řetězce viditelné pouze pro každý z nich zvlášť. Využití je tedy velice širokosáhlé a přínosné při správném nastavení práv pro čtení a různých práv pro různé typy transakcí.

1.5 Typy frameworků

1.5.1 Ethereum

Jedná se o jeden z prvních blockchain projektů, který je založený na decentralizovaných blockchain aplikacích s možností využití smart kontraktů. Jindy označovaný také jako blockchain druhé generace. Aby však bylo možné provozovat tuto síť, je nezbytné, aby obsahovala konsenzuální mechanismus Proof-of-Work s mining protokoly. Typickým využitím je tomu u Bitcoinu.

Ethereum je tvořeno Ethereum Virtual Machine (EVM), což je runtime prostředí. Toto prostředí běží na každém uzlu se spuštěnými skripty. Tyto skripty tvoří smart kontrakty, které je možné programovat a přidávat do nich různé podmínky, automatizovat dotazy a realizovat transakce inicializací jiné transakce.

V současné chvíli již existuje generace Ethereum 2.0, která uvádí do zmiňovaného projektu konsenzuální mechanismus Proof-of-Stake, který je vysvětlen v této práci níže. Nejde pouze o nástupce předcházejícího mechanismu, avšak také o zájem zvýšit bezpečnost Etherea, zvýšení procesování transakcí a rozšíření kapacity sítě.

1.5.2 Holochain

Jedná se o vývojový aplikační framework peer-to-peer síťového protokolu. Umožňuje vytvářet bez-serverové aplikace, které si zakládají na vysokém zabezpečení, výkonu a spolehlivosti. Uživatelé spouští aplikace na svém vlastním zařízení, generují vlastní data a komunikují přímo s ostatními uživateli.

Srovnání holochainu s dalšími přístupy v síti:

- Klient/server – existuje jeden centrální server, na který se jednotliví uživatelé připojují. Nevýhodou je, že pokud není server správně zabezpečen, je vystaven řadě zranitelností, a to jak na úrovni infrastruktury, tak operačního systému a aplikací na něm provozovaných. Uživatelé mezi sebou nijak neinteragují a komunikují výhradně se serverem.
- Blockchain – provádí distribuované výpočty a transakce za pomocí sítě uživatelů, jenž drží veřejné kopie datových sad. Každý z uživatelů zapojený do konkrétního blockchainu tak napomáhá udržet integritu a dostupnost dat. Vzhledem k tomu, že se jedná o decentralizovaný systém, chyby v zabezpečení jsou tak odstraněny. Nicméně někdy je velice nákladná replikace, kontrola a dosažení shody ve vztahu k datovým sadám.
- Holochain – se liší od blockchainu a klasického modelu klient/server tím, že celá myšlenka začíná u uživatele. Ti spouští modul holochainu a kopii back-endového kódu na svém zařízení, čímž přebírají zodpovědnost za řízení své identity a ukládání soukromých a veřejných dat. Vzhledem k provozu sítě peer-to-peer mohou účastníci vzájemně komunikovat a jsou taktéž vzájemně dohledatelní.

1.5.3 Solana

Tento typ projektu ve formě open-source frameworku s důrazem na vysoký výkon a typem permissionless blockchain sítě byl založen v Ženevě ve Švýcarsku jako Solana Foundation. Jedná se o centralizovanou databázi, která ve svém výkonu zvládne zpracovat 710 000 transakcí za sekundu v gigabitové síti za předpokladu, že průměrná velikost transakce činí více než 176 bajtů.

Projekt Solana funguje na principu clusteru, což je sada počítačů, která se zvenčí jeví jako jeden systém. Jednotlivé počítače zapojené do clusteru spolupracují navzájem (někdy i proti sobě), aby tak ověřili případné nedůvěryhodné programy odesílané uživateli. Jeho

uplatnění nalezneme v případě, kdy chceme uchovat záznamy událostí v časové ose, případně interpretace programů těchto událostí. Jednou z možností využití pro monitorování aktivit může být sledování vlastnictví aktiv, dále monitoring jednotlivých počítačů provádějících inkriminované úkony pro zajištění provozu clusteru. Uložené záznamy do clusteru jsou uchovány po celou dobu jeho životnosti. Konkrétní cluster je také znovu reprodukovatelný s obsahem všech záznamů, a to za předpokladu, že někdo udržuje kopii této hlavní knihy, bez ohledu na společnost, která jej prvotně spustila.

1.5.4 Hyperledger

Je open-source projekt založený společností Linux. Díky jeho platformě a typu licence jej využívají nadnárodní společnosti jako SAP, IBM a Intel. Tyto společnosti se snaží podpořit rozvoj a uplatnění technologie blockchain v průmyslu. Mezi základní pilíře filozofie projektu Hyperledger patří:

- Modularita – obsahuje jednotlivé modulární rámce, které je možné na základě jednotlivých bloků rozšiřovat a znovu použít. Tento přístup umožňuje vývojářům experimentovat s jednotlivými typy komponent bez toho, aniž by ovlivnily jakýmkoliv způsobem celý systém. Nastavený přístup modularity umožňuje jednotlivým týmům vývojářů pracovat nezávisle na sobě za použití stejných modulů s různými výstupy. Následně se mohou vrátit zpět k originálnímu modulu, který mohou dále přepracovávat pro různé projekty a účely.
- Vysoké zabezpečení – hraje klíčovou roli, neboť skrze blockchain a implementované frameworky proudí velký objem citlivých transakcí a dat. Velké objemy dat a velké množství uzlů jsou zajímavé pro online útočníky. Tyto uzly a data tvoří jednu velkou tzv. distribuovanou účetní knihu, která obsahuje žádané informace. Z tohoto důvodu jsou všechny protokoly, algoritmy a kryptografie Hyperledger kontrolovány bezpečnostními experty, a to v pravidelných intervalech.
- Interoperabilita – tak jak se blockchain sítě budou stávat běžnější součástí kritické infrastruktury, bude potřeba zajistit možnost vyměňovat si mezi nimi data. Tím se vytvoří složitější a výkonnější sítě. Takový přístup pomůže zvýšit zájem o tento typ spolupráce mezi nimi a zajištění požadované interoperability.

- Agnostický přístup ke kryptoměnám – základní filozofií Hyperledger je poskytnout možnost vytvořit blockchainový software pro podniky. Nicméně nesmí bránit tomu, aby jej různé subjekty mohly použít ke správě digitálních objektů, kterými mohou být právě i kryptoměny.
- Plná podpora API – všechny projekty Hyperledger poskytují snadno rozšiřitelná rozhraní API. Tato rozhraní umožňují snadnou interoperabilitu s ostatními systémy. Definovaná API sada umožňuje jasné pokyny a standardy pro komunikaci s ostatními externími systémy a hlavní infrastrukturou. Na základě rozhraní API umožňuje spolupráci, komunikaci a rozšiřování ekosystému a nabízí nové možnosti využití v průmyslu.

1.6 Konsenzuální mechanismy

Transakce je schválena za předpokladu, že uzly dosáhnou konsenzu s hlavní účetní knihou [3]. Tato definice je důležitá pro správné fungování blockchain sítě. To však není vždy lehké v případě, kdy je do ní zapojeno několik tisíc uzlů a všechny se mají shodnout na jednotném postupu a zásadách. O to obtížněji se této shody dosahuje, kdy celá myšlenka fungování blockchainu je založena na decentralizaci. Proto bylo potřeba vytvořit předem definované mechanismy, které jsou zabudované do blockchain sítě a umožňují tak dosáhnout shody i přes ohromný počet uzlů. Jednotlivé mechanismy jsou popsány níže. Vzhledem k různým typům sítí jsou tak i různé typy mechanismů, které jsou vhodné pouze pro některé z nich.

1.6.1 Proof of Work

Jedná se o zcela první algoritmus pro dosažení konsenzu mezi uzly. Vzhledem k tomu, že první algoritmus vznikl s blockchainem a kryptoměnou, jeho významem bylo zpracovávat náročné matematické úkony. Šlo zde o ověřování validity hlaviček bloku pomocí výpočtu hashe.

1.6.2 Proof of Stake

Tento konsenzuální algoritmus je vývojovým pokrokem z Proof-of-Work. Jeho princip je poněkud odlišný a nadto není tak energeticky náročný. Jeho základem je míra investované kryptoměny, nikoliv míra sdíleného výpočetního výkonu. Lze tedy

předpokládat, že je možné chápat Proof-of-Stake jako bezpečnější. Myšlenka je tedy taková, že uživatelé v síti blockchain na principu tohoto algoritmu investují. Uživatel, který více investuje, bude chtít, aby uspěl, tedy nebude mít zájem na jeho zneužití. Avšak aplikace tohoto algoritmu se může v každé síti lišit.

1.6.3 Proof of Authority

Jedná se o algoritmus fungující na principu ověření skutečné identity uzlů. Základem je možnost ověření identity v rámci daného blockchainu. Vzhledem k potřebě ověřit identitu a tím prokázat důvěryhodnost, se často používá tento konsenzus v privátních blockchainových sítích. Princip spočívá ve smyslu validace bloků pomocí identity.

1.6.4 Proof of Elapsed Time

Neboli PoET se využívá nejčastěji na privátních platformách, jež byly vyvinuty společností Intel v roce 2016. Jako základ tohoto konsenzu si společnost Intel stanovila za cíl jeho jednoduchost. Unikátní je především tím, že na rozdíl od ostatních algoritmů určuje pořadí uzlům a definuje, jak budou přidávat nové bloky za pomocí náhodného výběru. V první řadě se však všem ostatním uzlům oznámí doba čekání pro každého z nich. Počátek určuje první uzel s nejkratší dobou čekání, který provede přidání nového uzlu a následně informuje další uzly. Může však nastat situace, kdy dojde k přiřazení stejné doby čekání pro více než jeden uzel. V tento moment se vybere uzel náhodně a ten dostane přednostní právo zveřejnit nový blok.

I zde je potřeba zajistit bezpečnost daného algoritmu a znemožnit narušení procesu, který by zapříčinil přidání nového bloku pomocí zmanipulování nejkratšího času pro čekání uveřejnění nového bloku konkrétním uzlem. Společnost Intel proto upřednostnila spouštění algoritmu ve speciálním prostředí. Toto prostředí není spjato s operačním systémem, a tedy není možné upravovat či měnit chod konsenzuálního algoritmu. Proto se pro zesílení ochrany PoET používá specifická sada instrukcí procesoru v prostředí Safe Guard Extension k tomuto účelu určenému.

2 Bezpečnost

Užívání šifrovací a dešifrovací metody umožňuje zajistit integritu a autenticitu posílaných dat. Distribuovaný systém peer-to-peer se zabývá velkým množstvím dat a transakcí [4], a proto v technologii blockchain je používána k tomuto účelu asymetrická kryptografie. Pro šifrování se používá veřejný klíč a pro dešifrování soukromý klíč. Princip je takový, že z veřejného klíče, který může být znám komukoliv, se vygeneruje klíč soukromý. Tedy kdokoliv může zprávu veřejným klíčem zašifrovat, ale dešifrování je možné pouze klíčem vygenerovaným z klíče veřejného, jehož držitel je zároveň jeho vydavatelem. Na rozdíl od veřejného klíče je však privátní klíč držen v tajnosti a neměl by být sdílen.

V principu existují dva způsoby, jak se oba klíče používají:

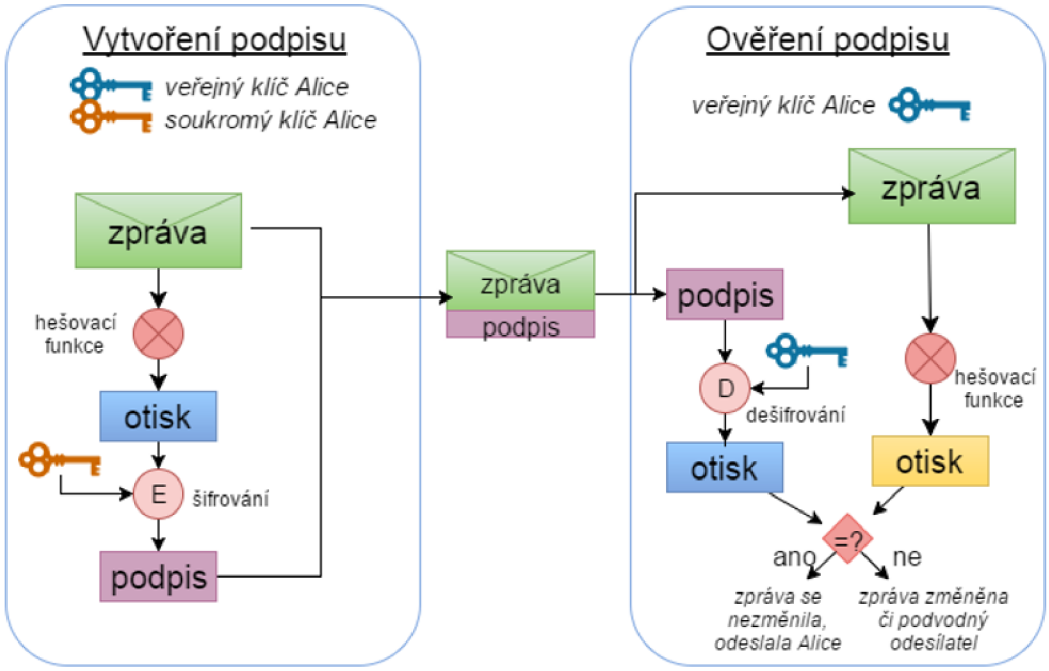
a) public-to-private

   V tomto případě je platné pravidlo zmíněné v úvodním odstavci této kapitoly, tedy veřejný klíč je používán k zašifrování, naopak k dešifrování se používá klíč privátní.

   Vzhledem k tomu, že privátní klíč drží pouze příjemce, není možné zprávu dešifrovat, i kdyby byla zachycena třetí stranou. Dnes se jedná o běžně používanou metodu pro šifrování emailové komunikace, například v bankách a jiných institucích, které jsou pod dohledem příslušných vládních orgánů požadující jistou úroveň ochrany dat při manipulaci a jejich přenosu.

b) private-to-public

   V případě této metody je princip obrácený, tedy veřejný klíč slouží k dešifrování, zatímco privátní klíč k šifrování odesílané zprávy či dat. Šifrovaná zpráva může být tedy přečtena kýmkoliv, kdo má veřejný klíč.



Obr. 2.1 Šifrování a dešifrování podpisu

Zdroj: [5].

2.1 Kryptografické hashovací funkce

Nezbytným parametrem v technologii blockchain je hashovací funkce. Jsou to malé počítačové programy, které transformují jakýkoliv druh dat na několik pevných délek bez ohledu na jejich vstupní velikost [4]. Za pomoci matematické funkce a procesem hashování vzniká hash. Takových hashovacích funkcí existuje nespočet a liší se pouze délkou hashe a způsobem výpočtu algoritmu.

Příkladem bezpečné hashovací funkce můžeme uvést SHA-512. Jeho primárním základem je generování hashe o velikosti 512 bitů, což je v podstatně obdoba SHA-256 s podobným principem výpočtu, která se liší pouze počtem kroků, odlišností konstanty a nelineárních funkcí. Následující obrázek znázorňuje postup výpočtu hodnoty hash, za podmínky znalosti proměnné hodnoty „data_size“, jejíž výsledek je uložen jako „result“.

```
byte[] data = new byte[DATA_SIZE];
byte[] result;
SHA512 shaM = new SHA512Managed();
result = shaM.ComputeHash(data);
```

Obr. 2.2 Příklad kódu hashovací funkce

Zdroj: [6].

Výhody hashovací funkce:

- univerzálnost – lze aplikovat pro jakýkoliv typ dat,
- antikoliznost – nikdy nemůže nastat situace, kdy hashovací funkce vyprodukuje dva identické výstupní hashe pro více sad vstupních dat,
- jednosměrnost – z výstupu je nemožné, ať už matematicky či výpočetně, získat vstup, naopak ze vstupu získat výstup je velice rychlé, neboť se nejedná o reverzní pokus prolomení hashovací funkce a kompromitaci dat,
- rychlost – šifrování a dešifrování je velice rychlé a efektivní,
- náhodnost – hashovací funkce s vysokým zabezpečením by měly produkovat velice odlišné hashe, a to i za předpokladu odlišnosti mezi vstupními daty, byť jen o pár bitů,
- konstantnost délky – bez ohledu na to, jak objemná jsou vstupní data, délka hashe bude vždy pro konkrétní hashovací funkci stejná. Toto je velice přívětivé v případě porovnávání identičnosti databází, které jsou zálohovány ve velkých datových centrech. Neporovnávají se data, ale shoda hashe, který slouží jako důkaz identičnosti.

Hashovací funkce v blockchainu:

- hash dat a digitální podpis – určují platnost a integritu dat transakce,
- hash a jednotlivé bloky – jsou na sebe jednotlivě vázány hashem,
- adresy v blockchainu – vychází z hashování veřejných klíčů a zajišťují, aby nedocházelo k totožnosti hashe pro více adres a tím nenastávaly kolize v systému.

2.2 Asymetrická kryptografie

Jedná se o primární využití kryptografie v blockchainu, jež zajišťuje bezpečnost mezi komunikujícími stranami, které se vzájemně neznají. V této kryptografii se využívá soukromý a veřejný klíč. Oba tyto klíče společně souvisí a jsou od sebe matematicky odvozeny. V oblasti blockchainu je primárně využívána k digitálnímu podpisu transakcí a zajištění jejich pravosti.

Proces užití asymetrického šifrování a souvisejícího páru klíčů začíná podepsáním transakce a jejím následným ověřením, které připadá uzlům v síti blockchain. Ověřování

takových transakcí je úkolem tzv. plných uzlů, tedy takových, které drží kopii blockchainové databáze. K zašifrování dat trasakce je potřeba, aby odesílatel vygeneroval hash těchto dat a ty následně digitálně podepsal privátním klíčem. Po tomto úkonu je možné data bezpečně odeslat. Takto odeslaná transakce je přijata příjemcem, který transakci ověří. K tomu je potřeba provést dešifrování pomocí veřejného klíče odesílatele. Po dokončení procesu je zobrazen hash šifrovaných dat. Následně při použití stejné hashovací funkce na přijatá data porovná generovaný hash s hashem přijatým při dešifrování podpisu. Pokud dojde ke shodě hodnot hashe, může příjemce prohlásit pravost dat a vyloučit tak jakoukoliv manipulaci během jejich přenosu.

2.3 Hashovací vzorce

V oboru kryptografie existuje řada známých a ustálených hashovacích vzorců, které se aplikují také v oblasti využití blockchainu pro zajištění integrity, validity a důvěryhodnosti dat. To znamená, že každá nezávislá část dat má svou vlastní jedinečnou kryptografickou hodnotu hash [4]. Mezi známé typy hashovacích vzorců patří:

Nezávislé hashování

Při využití tohoto vzorce dochází k rozdělení dat na menší jednotky, které se následně samostatně hashují. Výsledkem jsou pak jednotlivé datové celky s vlastním hashem. I skutečnost, že princip rozdělování dat na menší jednotky se může zdát jako nelogický, v kryptografii má tento vzorec své uplatnění. Díky rozdělení dat na menší celky lze následně lépe a rychleji v těchto datech vyhledávat. Princip je spojen se sestavováním hashovacích tabulek, ve kterých dochází následně k vyhledávání konkrétních dat.

Obr. 2.3 Nezávislé hashování

Zdroj: vlastní zpracování.

Opakované hashování

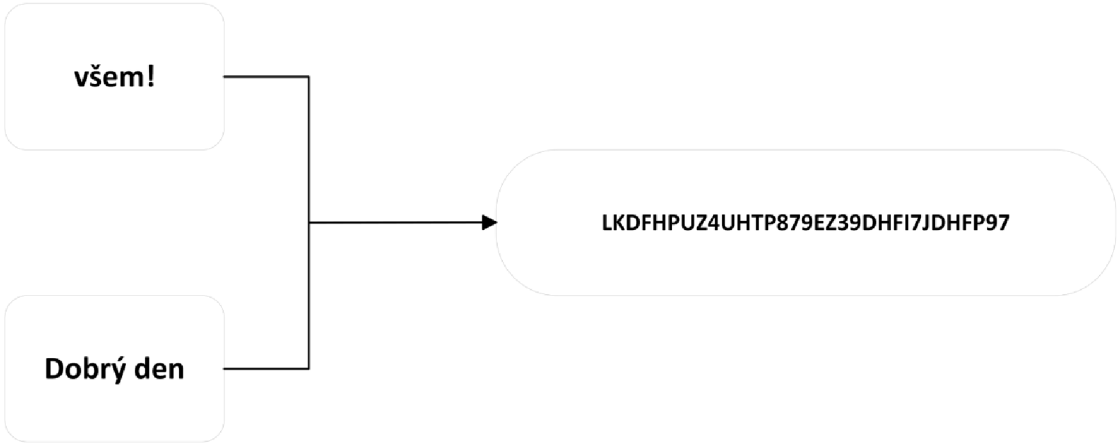
Spočívá v principu opakovaného hashovaní už jednou hashovaných dat. Jde o zesílení hashe. Typickým příkladem užití je ukládání různých přihlašovacích hesel, která jsou následně uložena v databázi u profilu uživatele.

Obr. 2.4 Opakované hashování

Zdroj: vlastní zpracování.

Kombinované hashování

Aby se neobjevovalo několik hashů pro více vstupů dat, je aplikováno kombinované hashování. Při využití tohoto principu dojde ke sloučení dat do jednoho celku a následnému hashování. Nachází se zde tedy pouze jeden řetězec dat s jedním hashem. Vzhledem k náročnosti interpolace dat je tato metoda náročná pro výpočetní výkon.

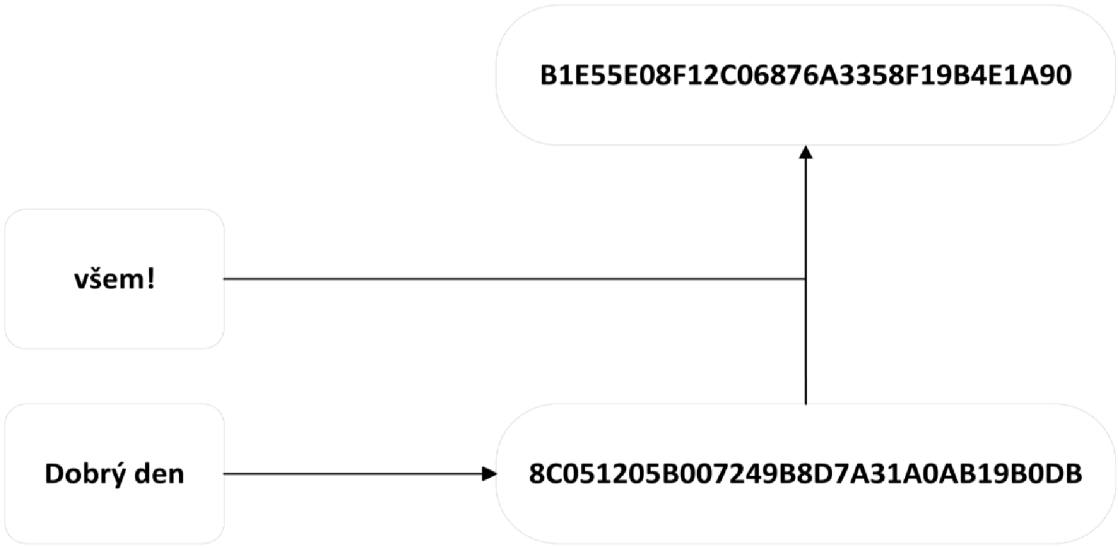


Obr. 2.5 Kombinované hashování

Zdroj: vlastní zpracování.

Sekvenční hashování

Jedná se o sloučení dvou typů hashovacích metod, konkrétně kombinovaného a opakovaného hashování. Princip spočívá v hashování nových dat, kdy původní data jsou hashována. Následně jsou přijata nová data, jež jsou přidána k původnímu hash řetězci a znovu hashována. Takto dojde k získání nového platného hashe zahrnující aktuální a původní data.

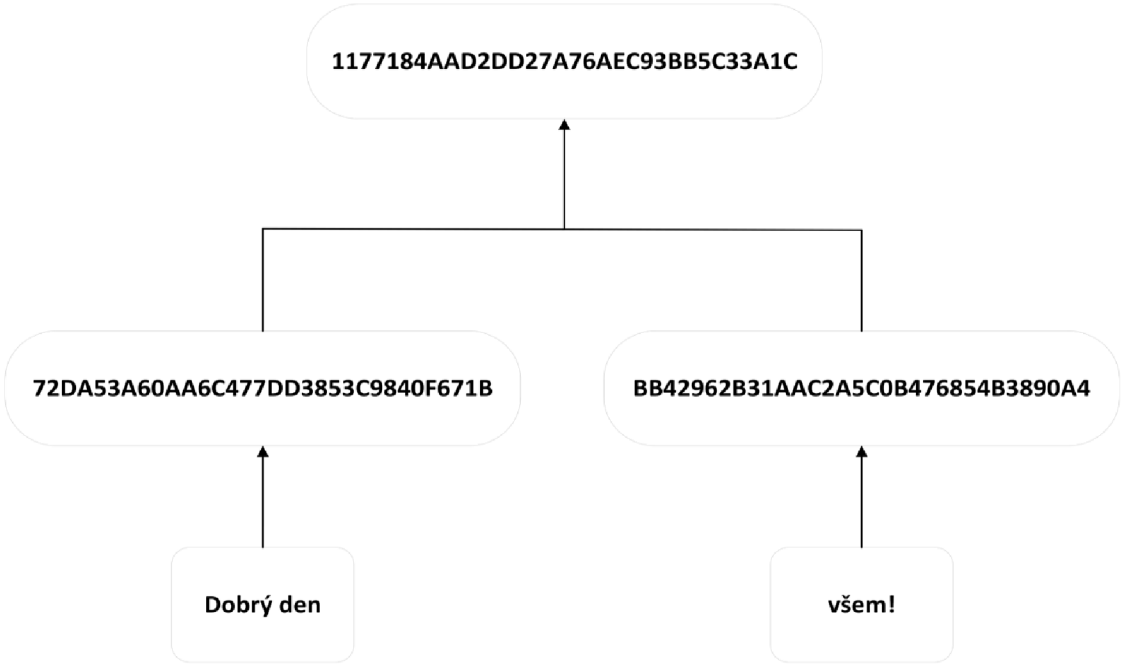


Obr. 2.6 Sekvenční hashování

Zdroj: vlastní zpracování.

Hierarchické hashování

Tento typ hashování je aplikován v případě Merkle Tree datové struktury, která provádí postupné hashování jednotlivých částí až dojde k úplnému zašifrování do jediné hashe. Data se hashují po částech a vzniklé hashe se dále hashuji do skupiny hashů, a takto se pokračuje zespoda nahoru v rámci stromové struktury. Výsledkem je níže popsaný jediný hash.



Obr. 2.7 Hierarchické hashování

Zdroj: vlastní zpracování.

2.4 ECDSA

Je typicky používaným algoritmem digitálního podpisu v technologii blockchain, který aplikuje vlastnosti eliptických křivek. ECDSA je standardizován několika normalizačními organizacemi a v současné době je vnímám stejně tak jako normy ANSI, IEEE, NIST a ISO [7]. Mezi algoritmy digitálního podpisu a šifrování za použití asymetrické kryptografie jsou velice obdobné spojitosti v oblasti faktorizace, diskrétního logaritmu a eliptických křivek. Nicméně úkolem digitálního podpisu, tedy ECDSA, je zaručit integritu a původ dat. Šifrovací algoritmy mají za úkol garantovat pouze původ dat za pomocí jejich šifrování.

3 Architektura

Základem architektury blockchainu jsou řetězce složené z jednotlivých bloků, které na sebe navazují. Každý blok obsahuje nosnou informaci neboli transakci, která je po zápisu neměnná a její parita je svázána přímo s hashem předcházejícího bloku. Tedy jde o užití kryptografie a aplikaci na jednotlivé bloky.

3.1 Blockchainový protokol

Stanovuje parametry blockchain programu a tvoří jeho jádro. V protokolu je zanesena stanovená informace o velikosti bloku a typ konsenzuálního algoritmu. Tento protokol však může být změněn, a to pomocí metody soft nebo hard forks. Metoda forks se však aplikuje pouze ve veřejné blockchain síti. V případě privátní blockchain sítě se jedná o změnu protokolu a algoritmu za pomoci dynamického řízení a nastavování.

3.2 Blok

Tak jako jakákoliv síťová komunikace se řídí protokoly a tyto protokoly mají v sobě zapouzdřené přesné schéma a data, jinak tomu není ani u technologie blockchain. Jednotlivé bloky, které jsou zapojeny do řetězců, mají identické schéma, a to hlavičku daného bloku a tělo bloku. Zatímco tělo bloku nese autorizované transakce, informace o jejich celkovém počtu v bloku a další data, hlavička bloku nese v přesně definovaných polích informace k zajištění integrity odeslaných dat. Mezi její metadata patří:

- verze bloku,
- hash s hodnotou předchozí hlavičky bloku,
- časový otisk vzniku bloku – slouží jako identifikátor přidání bloku do blockchain sítě,
- nBits – aplikovaná obtížnost použitá při vytváření nového bloku,
- nonce (number used once) – 32bitové číslo sloužící pro výpočet nového bloku zvyšující se po každé iteraci,
- hash Merkle Tree.

3.3 Merkle Tree

Jedná se o datovou strukturu, která je založena na hashování. Merkle Tree je mechanismus zajišťující ochranu proti manipulaci s datovými soubory v blockchainu. Pomocí této datové struktury jsme schopni velice rychle ověřit integritu dat bez toho, aniž by bylo potřeba všechny transakce jednotlivě kontrolovat.

3.4 Fork

Tak jako všechny systémy a jejich logika, i blockchain může procházet změnami parametrů a přijetím nových pravidel. Jde o termín, kdy projekt kryptoměny nebo tokenu potřebuje provést technickou aktualizaci vlastního kódu [8]. V takovém případě dochází k rozdvojení blockchain řetězce. Toto rozdvojení se označuje jako fork blockchainu. Aby však byla zachována integrita transakcí, jde vždy o předem naplánované aktivity. Dle vykonané změny existuje:

- Soft fork – představuje menší zásah a úpravu nastavených pravidel. Většinou se jedná o změnu velikosti bloku a časovou smyčku vytváření bloku. Výhodou soft forku je především ve zpětné kompatibilitě, a to díky přechodu celé sítě na nová pravidla, která se začnou uplatňovat.
- Hard fork – u tohoto typu forku dochází k reálnému rozvětvení v určitém bodě na základě dohody. Starý řetězec pokračuje stále dle dohodnutých pravidel, zatímco nový pokračuje odděleně s novou logikou.

Forky nejsou záležitostí, které by se používaly zřídka či vůbec. Téměř vždy v určitou dobu je potřeba přijmout nová pravidla, která způsobí změnu řetězce, či mají na něj přímý dopad, který změnu vyvolá.

3.5 Uzly

Každé zařízení, které je možné připojit k internetu disponující vlastní IP adresou, se může stát součástí blockchainové sítě. Takové zařízení se stane uzlem ve chvíli, kdy má v blockchainu přidělenou úlohu. Typickým uzlem je zařízení nebo počítačová stanice uživatele, kterou využívá v síti blockchain, a zároveň může zapůjčit svůj výpočetní výkon.

Tyto uzly jsou tedy různé dle své úlohy:

- Lightweight Nodes – tento typ uzlů validuje pouze transakce a bloky. Dále tyto transakce přenášejí a přijímají. Tyto uzly mají přímou závislost na Full Nodes a díky těmto uzlům dochází k interakcím s ostatními uzly. Jsou jakýmisi pomocníky bez poskytování infrastruktury.
- Full Nodes – jsou stěžejními prvky blockchain sítě, protože dodávají fyzický výpočetní výkon, tedy tvoří decentralizovanou síť blockchainu. Full Nodes obsahují jejich plnou kopii, přidávají nové bloky a kontrolují, zdali vše běží v souladu s nastavenými algoritmy.
- Routery – jejich úlohou je akvizice nových uzlů a přenos jednotlivých transakcí z jednoho účtu na druhý.

4 Využití blockchainu

Blockchain a jeho aplikování v praxi lze demonstrovat napříč mnoha odvětvími, které nám umožňují zvýšit efektivitu a zavést moderní metody. Bez ohledu na obor lze říci, že v každém případě je možné vydefinovat v konkrétních odvětvích oblasti, které dokážou specifika blockchainu využít.

Jeho uplatnění v odvětvích nás odkazuje zpravidla do dynamicky řízených sítí v privátním blockchainu, které lze rozvíjet v korporacích v různých odvětvích podnikání.

4.1 Logistika

Zrychlující se globalizace a komplexita dodavatelských řetězců má klíčový dopad na mezinárodní společnosti. Zúčastněné strany logistického řetězce potřebují zpracovávat zvyšující se objem informací za souběžného držení záznamů o výkonu a plánování budoucích aktivit běžícího řetězce. Logistické procesy zahrnují několik subjektů vyžadujících vzájemnou spolupráci napříč každým procesem. V dnešní době je však spolupráce většinou vedena manuálně či asynchronně, což často vede k nadbytečnosti procesů a chybám. Proto technologie blockchain může pomoci zmírnit mnoho kritických procesů a zlepšit logistiku globálního obchodu zahrnující nákup, řízení dopravy, sledování zásilky a její trasy, konsenzus spolupráce a financování obchodu [9]. K významné efektivitě však dojde teprve tehdy, pakliže všechny kooperující strany procesu budou společně sdílet data k vytvoření efektivity a transparentnosti procesu. Klíčové prvky, ve kterých logistika čelí výzvám ve sdílení informací napříč celým dodavatelským spektrem, jsou relevantní v několika směrech:

I. transparentnost – tok informací přispívající k podpoře plánování a kontroly uvnitř dodavatelského řetězce,
II. rychlost a efektivita – zajištění doručení správného zboží na správné místo určení a v pravý čas za pomocí digitalizovaných a efektivních procesů,
III. sledovatelnost – zajištění spolehlivého sledování a pohybu zboží a materiálu v každé fázi dodavatelského řetězce zahrnující doklad o poloze, auditní stopě a certifikaci,
IV. platba – převody peněžních prostředků mezi dodavateli za podpory důvěryhodné dokumentace.

Logistika je velice dynamické a klíčové prostředí zajišťující přepravu hotových výrobků a materiálu. Díky jejímu nastavení a propracovanému systému je celý svět v pohybu. Jinými slovy, bez logistiky bychom nebyli schopni produkce, jako je tomu dnes. Avšak i taková produkce potřebuje neustále zlepšovat své procesy. Nároky a technologie jdou kupředu, a proto již dnes nestačí logisticky zajistit přesun zásilky z bodu A do bodu B. Nově je potřeba sledovat jeho průběh cesty, u potravin to naopak může být způsob zacházení a podmínky přepravy. Tyto požadavky jsou totiž kladeny dohledovými orgány, odběrateli a v některých případech i koncovými spotřebiteli. Než se tedy dostane zásilka k cílovému bodu, projde celým dodavatelským řetězcem, od velkoobchodníků, maloobchodníků, přepravců a různých distributorů.

Důvody pro inovace jsou jednoduché, a to snížení administrativy, zvýšení efektivity, a především inovování procesů k urychlení doručení zásilky a dalších procesů v oblasti logistiky.

V neposlední řadě, motivací využití technologie blockchain v logistice a dodavatelských řetězcích je faktická různorodost zaznamenávaných informací, odlišnost platforem a nekonzistentnost. Toto samo o sobě ve většině případů neumožňuje fungovat v celistvém systému, který by integroval informace jednoduše mezi jednotlivými subjekty logistiky a dodavateli.

Výhody blockchainu v logistice:

a) Transparentnost a sledování dodavatelského řetězce
    - Transparentnost mezi koncovými body – v logistice poskytuje blockchain jedinečný zdroj validních dat za pomoci jejich integrace od všech účastníků dodavatelského řetězce.
    - Sledování výkonu – monitorování za pomocí blockchainu poskytuje přehled informací o historickém výkonu důvěryhodných dopravců a dodavatelů.
    - Potvrzení původu – společně s prokazatelností původu, blockchain poskytuje taktéž ujištění o dodržování všech předpisů a bezpečnostních standardů napříč dodavatelským řetězcem.

- Sledování v reálném čase – transparentnost blockchain řešení aplikovaného v logistice poskytuje informace o událostech a statusech v reálném čase bez ohledu na druh dopravy.

b) Bezpečnost a autenticita
   - Ověření údajů a dokumentů – vzhledem k charakteru dosažené platnosti dat prostřednictvím aplikované kryptografie, blockchain je bezpečnou a šifrovanou platformou pro výměnu dat a dokumentů.
   - Odhalení podvodů – všechny transakce zaznamenané v síti blockchain jsou viditelné pro všechny účastníky sítě a žádná z dříve schválených a uveřejněných transakcí nemůže být zpětně odstraněna bez toho, aniž by si toho žádný z účastníků nevšiml. Princip fungování sám o sobě brání výskytu podvodného jednání.
   - Předcházení krádeži – nastavení systému může představovat takové zásady, které zabrání neoprávněnému převzetí zásilky na základě pravidel a požadovaných informací při předání příjemci, které zvyšují bezpečnost a snižují nedovolené přivlastnění.

c) Složitost procesu
   - Minimalizace zprostředkovatelů – využití blockchainu nahrazuje řadu zprostředkovatelů v ekosystému logistiky za pomocí důvěryhodnosti, které řešení přináší. Umožňuje aplikování modelu peer-to-peer.
   - Zajištění zlepšování kvality – vzhledem k množství platných dat, které jsou v rámci procesu přidávány do sítě, mohou být dále vyhodnocována a ověřována. Lze tedy posoudit zásilku na vstupu a výstupu při doručení. Toto pomáhá eliminovat případné stížnosti a jejich řešení.
   - Zvyšování úrovně automatizace – pomocí chytrých kontraktů lze automatizovat řadu činností, které jsou napsané v počítačovém kódu. Těmito procesy mohou být platby, různé smluvní převody či v logistice přímo kontrola nákladu.

d) Provozní efektivita
   - Zajištění zlepšování předpisů – využití blockchainu může být kombinováno s řadou aplikací, které přispívají k vytěžování užitečných dat a jejich následnému vyhodnocování. V logistice můžeme zmínit ELD,

který zasílá data z vozidla řidiče o jeho jízdním chování (doba odpočinku, rychlost, styl jízdy).

- Eliminace nákladů – je podmíněna principem ověření shody, jenž napomáhá blockchainu vyhnout se opakujícím transakcím a procesním chybám, které mohou nastat při ověřování správnosti transakce.
- Eliminace lidské chyby – vzhledem k automatizaci procesů pomocí chytrých kontraktů dochází taktéž ke snížení manuálních procesů, a tedy eliminaci lidské chyby, která by byla v takových to procesech vstupním faktorem.

4.2 Průmysl

4.2.1 ElA Blockchain

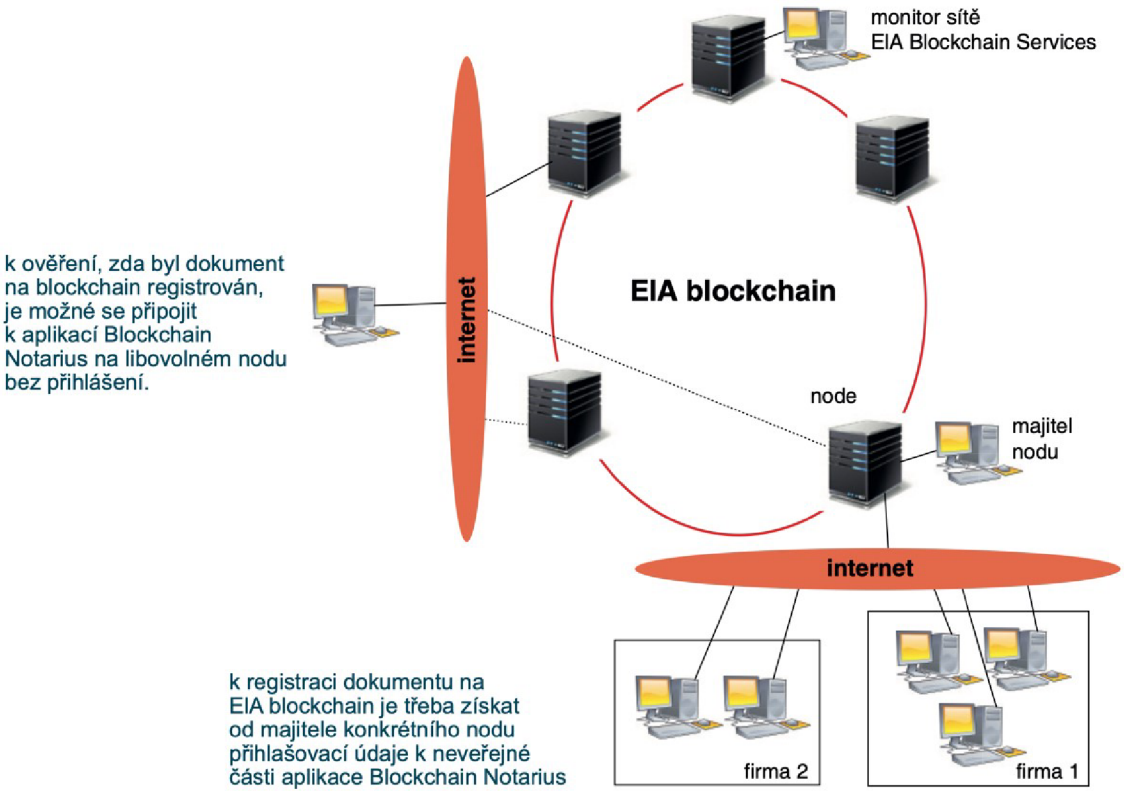
Jedná se o zastupujícího garanta pro zajištění kredibility právnickým subjektům, kterým je udělen elektronický certifikát představující identitu subjektu opravňující k operacím na ElA Blockchain. Zásadním principem ElA blockchainu je, že se do něj neukládají dokumenty, ale pouze jejich digitální otisky, tzv. hashe [10].

Tato platforma vznikla, aby podpořila průmysl, obchod a bankovnictví. Prostřednictvím ElA Blockchainu je možné ověřit certifikát, diplom, uzavírat smlouvy, odhalovat padělky a sledovat zboží. Jedná se o klíčovou technologii pro Průmysl 4.0 a záměrem je, aby na této platformě zájemci stavěli svá řešení.

Zásadní rozdíl mezi IBM, Maersk a dalšími nadnárodními korporacemi, které tyto blockchainové projekty financují, je fakt, že ElA Blockchain nemá centrálního zřizovatele. Je to pouze o dobrovolném zapojení majitelů nodů. Ti pro zajištění důvěryhodnosti vystupují jako právnické subjekty. Jednotlivé nody a jejich majitelé jsou veřejně dostupní. Externí uživatel si tak může sám vybrat, koho si zvolí jako důvěryhodnou autoritu pro ověřování listin a další úkony. Mezi základními pravidly je ustanoveno, že jeden právnický subjekt může provozovat pouze jeden nod. Takto se tato heterogenní síť stává vysoce odolnou vůči hackerskému útoku.

Smysl využití ElA Blockchain nezná hranice a není stanoven pro konkrétní typ aplikace. Jedna základní aplikace se však povinně musí nacházet na každém nodu, a to Blockchain

Notarius, která v sobě obsahuje ty nejběžnější blockchainové služby. V podstatě není možné využívat řešení ElA Blockchain bez Blockchain Notarius, ke kterému se přistupuje za pomocí webového prohlížeče. Zároveň na základě webové aplikace je možné ověřit a registrovat jakýkoliv dokument. Další výhodou je fakt, že nemusíte primárně vlastnit node, ale můžete se domluvit s majitelem nodu, který vám poskytne přístup za sjednanou pravidelnou platbu. Grafická podoba na obrázku níže vysvětluje princip ElA Blockchainu:



Obr. 4.1 Princip ElA Blockchainu

Zdroj: [8].

4.3 Dodavatelský řetězec

V dnešní vysoce produktivní době jsou k dispozici potraviny bez ohledu na roční období, prostředí nebo místo. Výrobci potravin po celém světě denně produkují výrobky a čerstvé zboží pocházející z rostlinné produkce a zvířecího zpracování. Tyto možnosti a neomezená dostupnost však zvyšuje složitost celého dodavatelského řetězce.

Důležitou roli hraje kvalita a čerstvost, která může být někdy pochybná. S narůstajícím objemem zpracovávaných dat a velkým množstvím dodavatelů je velice těžké sledovat každý poražený kus skotu a produkty z něj zpracované. Jinak tomu není ani u pěstovaných produktů pocházejících z přírodních rostlinných zdrojů. Velký tlak na produktivitu snižuje důvěřivost zákazníků mnohem více než kdykoliv předtím. Proto přišla společnost IBM s projektem IBM Food Trust, aby tak rozšířila aplikování blockchainu v dodavatelském odvětví a zajistila transparentnost procesu od farmáře, přes zpracovatele, obchodní řetězce až ke spotřebiteli. Tento přístup poskytuje nespočet možností využití v potravinovém odvětví, zvýšení důvěry u spotřebitele a transparentnosti mezi jednotlivými stranami obchodující s potravinami. Značnou výhodou je možnost přistupovat k doprovodným datům (údaje o testech, udělených certifikacích a skladovací teplotě).

4.3.1 Modularita

a) Zajištění efektivity dodavatelského řetězce – pomocí sofistikovaných procesů exekuovanými mezi potravinovými systémy jsme schopni identifikovat ty neefektivní. Přehledy potravinářských dat v blockchain řešení můžeme nastavit predikci poptávky, optimalizovat podnikání a tím zvýšit jeho růst.
b) Povědomí o značce – využitím blockchainu a poskytnutím dat pro zajištění transparentnosti je možné zvýšit povědomí o značce, její důvěryhodnost vůči spotřebitelům, ale také obchodním řetězcům.
c) Čerstvost potravin – data z dodavatelského řetězce poskytují poznatky a analýzy odkazující na kvalitu zboží.
d) Potravinové podvody – za pomoci zajištění plné digitalizace záznamů transakcí a jejich decentralizovanému a neměnnému ukládání se sníží riziko podvodů v potravinovém systému.
e) Udržitelnost – aplikovaní blockchainu v potravinovém odvětví umožňuje digitalizovat základní dokumenty a certifikáty, ukládat a optimalizovat informace. V neposlední řadě také ověřovat původ a autentičnost.

4.3.2 Sledování pohybu potravin v logistickém procesu

Řada států stanovuje dodavatelům a přepravcům legislativní rámce, které jsou navázané na normy, za jakých podmínek mají být potraviny přepravovány a skladovány

na překladištích. Rychlost a přesnost jsou dalším klíčovým faktorem, aby byl zajištěn soulad s globálními předpisy zaměřenými na bezpečnost potravin. Za pomoci blockchain řešení je možné ověřit jejich stav a dodržování, zobrazit umístění, bezpečnost a v neposlední řadě důvěryhodnost.

Ke sledování potravinářských produktů je potřeba, aby účastníci tohoto cyklu poskytli údaje o výrobcích do blockchain sítě. Po nahrání, trasovací modul umožní oprávněnému uživateli prozkoumat původ produktu, a to prostřednictvím GTIN (Global Trade Item Number) kódu. Toto hraje klíčovou roli, pakliže by došlo ke kontaminaci zásilky. Je možné rychle identifikovat problém a zamezit další kontaminaci a jejímu šíření. Když tedy shrneme výhody, můžeme uvést následující:

- ověření původu během několika sekund,
- schopnost zjištění kontaminace potravin a okamžitého zásahu,
- schopnost prokázat bezpečnost produktů separovaných od ohniska kontaminace,
- zvýšit důvěru a spokojenost zákazníka.

5 Návrh systémového využití v oblasti farmaceutického průmyslu pro distribuci vakcín proti SARS-COVID-2019

5.1 Řešený problém

Jeden ze současných problémů v době, kdy logistika hraje klíčovou roli, je oblast farmaceutického průmyslu. Jelikož zmíněný obor podléhá čím dál více nařízením jednotlivých vlád a Evropské unie, je potřeba dodržovat nikoliv jen stanovené požadavky, ale zajistit, aby skladování a přeprava byla v souladu s požadovanou kvalitou. O to důležitější roli hraje v situaci nedávné pandemie SARS-COVID-2019, která zmítá svět a farmaceutické společnosti jsou přinuceny čelit novým výzvám a komplikacím.

Bohužel vývoj očkovací látky má takové nároky z pohledu logistiky, že i ty největší společnosti vnímaly přepravu očkovací látky jako jednu z velkých výzev. Pro příklad vakcína od společnosti Pfizer/BioNTech má stanovenou skladovací teplotu -90 °C až -60 °C. I přes snahu vyhovět a dodržet tyto požadavky, není žádná jistota, která by prokazovala plnění stanovených parametrů, a tedy zachování potřebné kvality pro požadovanou účinnost. V této situaci se spoléháme pouze na výrobce, logistické přepravce a státní instituce v jejich tvrzení.

Dalším aspektem je padělání vakcín a černý obchod s jejich zásobami. Již se objevily vakcíny, které vypadaly věrohodně, avšak výrobce nepotvrdil jejich vydání. Vzhledem k tíživé situaci se tato očkovací látka stala velice lukrativním zbožím pro černý trh. Proto je nezbytné mít jistotu, že vakcína, která byla přijata koncovým zdravotním zařízením, bude pravá a její pravost bude ověřitelná. To však v současné chvíli nemůže nikdo s okamžitou možností ověření garantovat. Samozřejmě, zodpovědné instituce by sdělily, že taková situace nemůže nastat, ale případ ukázal, že to je možné a je tedy nezbytné tomuto zamezit pomocí technologií, které dnešní doba nabízí.

V neposlední řadě si každá farmaceutická společnost stanovuje výrobní postupy a procesy, které musí být v souladu s normami a požadavky státních institucí. Tuto dokumentaci sdílí na vyžádání s dohledovými orgány a případnými externími vědeckými týmy. Aby však bylo možné zajistit, že příslušná dokumentace je platná, je možné využít řešení ElA Blockchain zahrnující Blockchain Notarius.

5.2 Současné řešení

Nyní se spoléháme pouze na to, že všichni postupují dle norem, standardů a ověřených postupů, a to ve farmaceutickém průmyslu, logistice a jiných odvětvích. Nicméně nikde není možné dohledat konzistentní data o tomto postupu, či neexistuje zaběhnutý systém, který by to umožňoval. Možnosti tu jsou, avšak nejsou nastavené a zavedené do praxe. Blockchain je v logistice již známý, avšak farmaceutický průmysl neumí s tímto pojmem ve svém výrobním a logistickém procesu pracovat. Farmaceutické společnosti si samozřejmě vedou záznamy o vyrobených vakcínách, kontrolách kvality, ale neumí tato data propojit s koncovými zdravotními zařízeními, aby jim poskytly možnost k těmto datům přistupovat a nezávisle si konkrétní očkovací látku ověřit, a to od její výroby až po koncový bod logistického procesu.

V oblasti ověřování dokumentace není také bohužel proces nastaven tak, aby využil maximální potenciál současných možností v oblasti digitalizace. Dokumenty se sdílejí klasickou cestou přes šifrované emaily, nicméně je na příslušných úřadech, aby si ověřili stálou platnost příslušných výrobních a logistických procesů. Blockchain Notarius v ElA Blockchainu by umožnil tak během několika málo vteřin ověřit, zdali je dokumentace stále validní podle příslušného hashe uvedeného na distribuované dokumentaci.

5.3 Navrhované řešení

Využít blockchain pro sledování dodržení kvality při přepravě vakcín a současně ověření její pravosti je vhodným a smysluplným krokem, jak se posunout ve farmaceutickém průmyslu na další úroveň. Za pomocí blockchainu by mohly tyto společnosti sdílet se zdravotními zařízeními a státními institucemi podrobnosti o datu výroby, datu expirace, datu expedice, skladovací teplotě během uskladnění a přepravě až po převzetí zásilky centrálním vládním orgánem pro distribuci vakcín. V neposlední řadě by toto sloužilo jako automatické potvrzení o pravosti vakcíny na základě dostupných dat vztahující se ke konkrétní šarži.

Tímto záměrem lze demonstrovat využití blockchainu ve farmaceutickém průmyslu, který by zprostředkoval dostupná data výrobce směrem ke zdravotnickým zařízením. Inkriminované záznamy budou vždy uchovávány za pomocí blockchainu v distribuované

databázi. Tato data budou transparentní a neměnná. Její funkčnost bude postavena na blockchain open-source frameworku.

Pro zajištění pravosti výrobních a logistických procesů bude využit naopak ElA Blockchain a její aplikace Blockchain Notarius, který umožní během několika málo vteřin ověřit, zdali je dokumentace stále validní podle příslušného hashe uvedeného na distribuované dokumentaci.

6 Implementace

Cílem je vytvořit řešení za pomoci využití blockchainu pro sledování kvality a ověření pravosti ve farmaceutickém průmyslu. Vybraný problém by zaručil pravost a účinnost očkovací látky, jejíž padělek a případná špatná kvalita může být rizikem pro pacienta, kterému je očkovací látka aplikována. Zároveň se takto minimalizuje vakcinace sníženou kvalitou očkovací látky, která by tak nemusela zcela účinně chránit proti SARS-COVID-2019.

6.1 Výběr frameworku

Před samotnou implementací je důležité stanovit si Framework, na kterém bude blockchain síť fungovat a zároveň si definovat přesné parametry, které by měl systém splňovat.

- Jde o systém, který je kontrolovaný a pro zadávání dat má přístup pouze oprávněná osoba z farmaceutické společnosti. Ke transakcím mají přístup pouze vybraní zaměstnanci na straně zdravotního zařízení. Síť je tedy typu permissioned.
- Jelikož se jedná o využití pro sdílení dat na straně výrobce, framework je bez kryptoměny.

Při specifikování výše popsaných zásad, které má primárně framework splňovat, může vyloučit frameworky podobné Ethereum, Quorum, Corda. Jedná se totiž o frameworky, které se zaměřují na kryptoměny a finanční projekty. Jako ideální se však jeví Hyperledger a jeho známé varianty Hyperledger Fabric, Hyperledger Sawtooth a Hyperledger Grid. Pro potřeby této práce bude v rámci implementace využit Hyperledger Fabric. Jeho výhodou je dostačující dokumentace a možnost zabudované komunikace prostřednictvím REST API (jedná se rozhraní zajišťující komunikaci mezi aplikacemi) v případě využití Hyperledger Composer.

6.2 Hyperledger Composer

Jde o nástroj, který je napsaný v javascriptu a usnadňuje navrhování, vývoj a testování aplikací, které jsou vyvíjeny na Hyperledger Fabric. Zároveň umožňuje vytvoření REST API komunikačního spojení pro různá zařízení a webové stránky. Vzhledem k tomu, že

zdravotnický personál bude přistupovat k datům prostřednictvím zabezpečeného webového prostředí určeného pro konkrétní skupinu uživatelů, je ideální pro dané řešení.

6.3 Transakce v síti blockchain

Aby bylo možné s blockchain sítí pracovat, je nutné vytvořit systém, kdy se budou na webové stránce po zadání čísla šarže zobrazovat údaje o vakcíně. K tomu je potřeba definovat transakce, které budou obsahovat požadovaná data.

- originalitaVakciny – jedná se o transakci, která bude potvrzovat výrobu vakcíny příslušnou farmaceutickou společností,
- expiraceVakciny – transakce poskytuje informaci o datu expirace vyrobené vakcíny v konkrétní šarži,
- datumVyrobyVakciny – jde o klíčovou transakci, která poskytuje konkrétní datum výroby vakcíny a potvrzuje tedy její vhodné použití,
- datumExpediceVakciny – toto je první transakce poskytující informace o začátku logistického procesu v přepravě,
- teplota – poskytuje pouze informaci, zdali nedošlo v přepravě k porušení výrobcem stanovené přepravní teploty a pomocí funkce boolean vrací hodnotu „OK“ a „NOT OK“,
- prevzetiVakciny – po ukončení přepravy se doplní záznam o datu a času doručení a jméně zaměstnance přebírající zásilku,

6.4 Povolení

Vzhledem k tomu, že se jedná o permissioned blockchain síť s řízeným přístupem, je potřeba definovat přístup pro každého účastníka, tedy pro každý stát jeden účet. Přístupy jsou řízeny pomocí pravidel, která jsou součástí business network struktury konceptu Hyperledger Composer.

6.5 Objektové třídy

V konkrétním bodě návrhu je potřeba identifikovat klíčové objekty v navrhovaném systému. K tomu nám pomáhají popisy použití operací v systému a identifikace objektů.

Z níže identifikovaných objektových tříd je jasné, že se stanou klíčovými prvky reprezentující inkriminovaná data o vyrobených vakcínách. Tato data budou shromažďována, a dále zpracovávána objektem reprezentující souhrn těchto dat. Abychom konkrétní objekty mohli správně definovat, je potřeba užití vysokoúrovňového systému objektů, který zapouzdří systémové interakce. Poté, co jsou identifikované objekty, je možné identifikovat také objektové třídy.

6.5.1 Třída WebovyInformacniSystem

Jedná se o základní front-end rozhraní, ke kterému přistupujeme prostřednictvím webové stránky. Vykonávané operace odrážejí interakce vycházející ze slovního návrhu architektury níže v této práci. Veškeré interakce jsou zapouzdřené do jediné objektové třídy s názvem WebovyInformacniSystem. Jednotlivé objekty v této objektové třídě jsou základním požadavkem pro zajištění ověřování dat s autorizovaným přístupem prostřednictvím webového přístupu. Objekty této třídy jsou definované v tabulce níže:

Tab. 6.1 Objektová třída WebovyInformacniSystem

WebovyInformacniSystem
IDuzivatele heslo
prihlaseni (uzivatele) odhlaseni (uzivatele) cisloSarze odeslat (prikazy)

Zdroj: vlastní zpracování.

6.5.2 Třída VakcinData

Objektová třída VakcinData odpovídá za zpracování příkazu z objektové třídy WebovyInformacniSystem a její následné odpovědi. Odesílá tak poskytnutá souhrnná data pro konkrétní požadavek.

Vykonávané operace odrážejí interakce vycházející ze slovního návrhu architektury níže v této práci. Všechny interace jsou zapouzdřené do jediné objektové třídy s názvem WebovyInformacniSystem. Jednotlivé objekty v této objektové třídě jsou základním požadavkem pro zajištění ověřování dat s autorizovaným přístupem prostřednictvím webového přístupu. Tyto objekty jsou definované v tabulce níže:

Tab. 6.2 Objektová třída VakcinData

VakcinData
originalitaVakciny expiraceVakciny datumVyrobyVakciny datumExpediceVakciny teplota prevzetiVakciny
shromazdi () shrn ()

Zdroj: vlastní zpracování.

6.5.3 Třída SpravaZarizeniTeplomeru

Tato objektová třída je zodpovědná za správu jednotlivých zařízení elektronických teploměrů a jejich řídících jednotek umístěných ve speciálních přepravních vozech s mrazícími boxy. Tyto řídící jednotky fungují plně v online režimu a jsou schopny odesílat nashromážděná data a zároveň přijímat příkazy. Prostřednictvím těchto příkazů je možné vyvolat vzdálené řízení jednotky, změnu konfigurace a dále vypnutí/restart jednotky, tak jak je uvedeno v objektové třídě níže:

Tab. 6.3 Objektová třída SpravaZarizeniTeplomeru

SpravaZarizeniTeplomeru
Identifikator
oznamTeploty () oznamStav () vzdaleneRizeni (prikazy) zmenaKonfigurace (prikazy) restart (pristroje) vypnuti (pristroje)

Zdroj: vlastní zpracování.

6.5.4 Třída TeplomerPreprava

Objektová třída souvisí přímo se zařízeními v systému a odráží fyzické hardwarové prvky a jejich operace. Elektronický teploměr umístěný v přepravní části shromažďuje data automaticky, která následně poskytuje centrální jednotce teploměru. Ty posléze odesílá prostřednictvím mobilního internetového připojení do blockchain sítě farmaceutické

společnosti. Tato data jsou poskytována na základě příkazu odeslaného prostřednictvím webového přístupu po zadání čísla šarže vakcíny a jsou součástí zapouzdřených dat v odpovědi webové stránce, která má definovanou objektovou třídu WebovyInformacniSystem.

Tab. 6.4 Objektová třída TeplomerPreprava

TeplomerPreprava
tz_Ident teplota
nacti ()

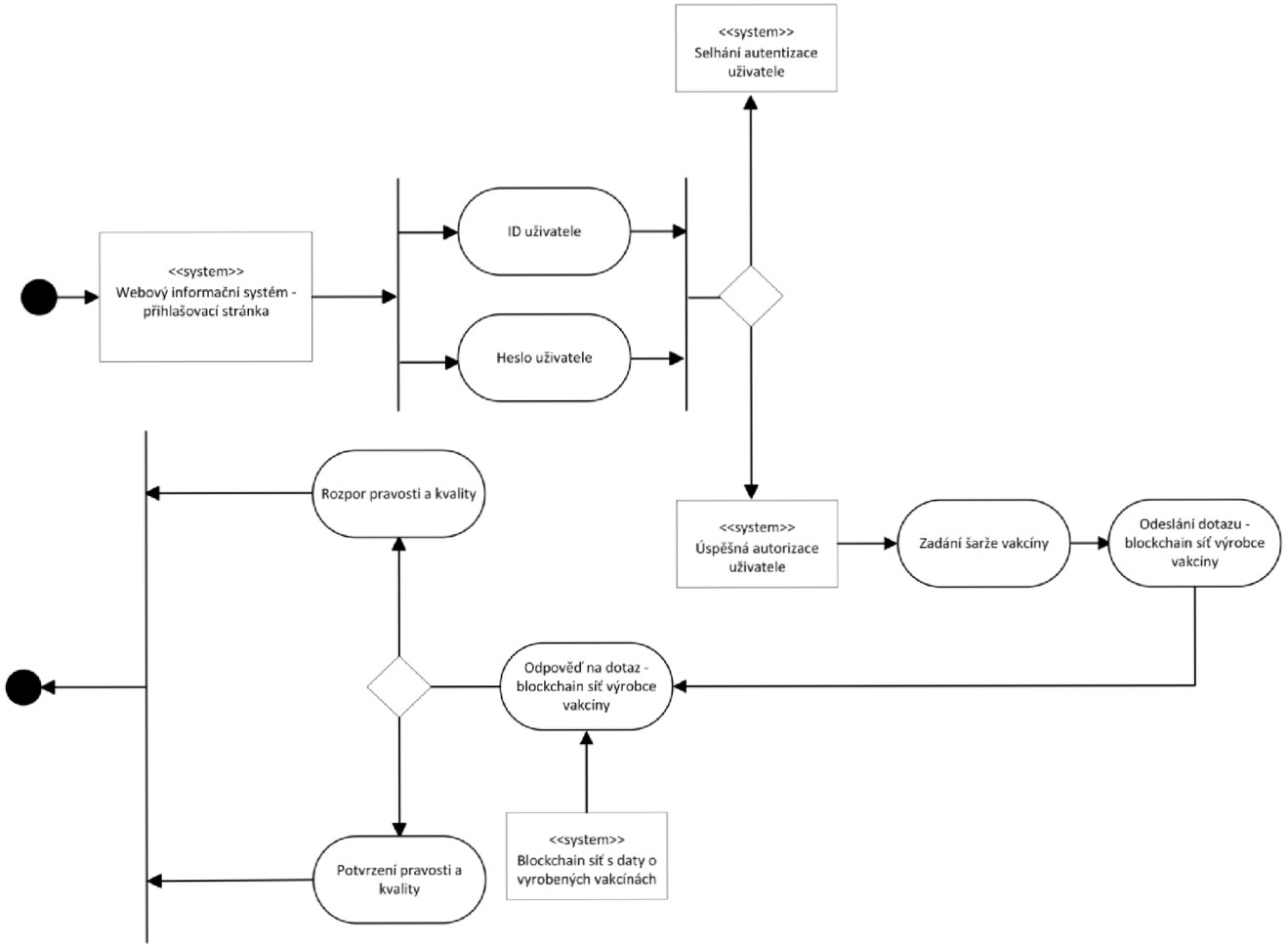
Zdroj: vlastní zpracování.

6.6 Systémové modelování

Umožňuje vytvářet abstraktní modely systému. Těchto modelů může být několik a každý poskytuje jiný úhel pohledu na daný systém. Mimo jiné také slouží pro klasifikaci silných a slabých stránek funkcionalit systému a definovaného modelu. Pro znázornění představy v tomto návrhu je využit Procesní model, který je pro dané znázornění nejlépe vyhovující. K vyhotovení modelu a dalších částí návrhu byl využit primární zdrojový pramen pro vypracování této práce [11].

6.6.1 Procesní model

Znázorňuje dotaz požadavku prostřednictvím webového informačního systému. Jde o dotaz prostřednictvím API do databáze k ověření dat v blockchain síti na straně farmaceutické společnosti. Slouží primárně k detailnímu dotazu vztahující se ke konkrétní šarži vyrobené vakcíny.



Obr. 6.1 Procesní model webového informačního systému

Zdroj: vlastní zpracování.

6.7 Návrh architektury

Aby bylo možné navrhnout funkční architekturu, je potřeba identifikovat hlavní komponenty a systémové interakce. Dosažení vhodného návrhu architektury je potřeba nejprve vytvořit popis případu jejího použití, ze kterého je následně možné zpracovat architektonický model.

6.7.1 Popis případu použití

Tab. 6.5 Popis případu použití pro návrh architektury

Systém	**Blockchain ve státní správě – zdravotní sféra a farmaceutickém průmyslu**
Případ použití	Ověření pravosti a kvality vakcíny
Aktéři	Systém blockchain ve státní správě zdravotního odvětví a dodavatelé vakcín
Data	Prostřednictvím systému blockchain přijímající zdravotní zařízení ověří dodávky vakcín proti SARS-COVID-19. Po načtení šarže balení jsou načtena z centrálního distribučního systému výrobce vakcíny data, která jsou k dispozici. Od výrobce se odešlou data potvrzující originalitu vakcíny, její expiraci, datum výroby, datum expedice z farmaceutického závodu, potvrzení o dodržení přepravní teploty a potvrzení o převzetí zásilky centrálním skladem pro distribuci vakcín.
Impulz	Informační webový front-end systém po autorizovaném přihlášení zdravotnického personálu nabídne načtení údajů po zadání čísla šarže z balení přijatých vakcín. Zadaná data pomocí blockchain systému ověří a dohledá příslušnou šarži. Toto ověření může být prováděno i dodatečně.
Odpověď	Souhrnná data jsou odeslána do webového rozhraní informačního systému.

Zdroj: vlastní zpracování.

6.7.2 Vrstevnatá architektura

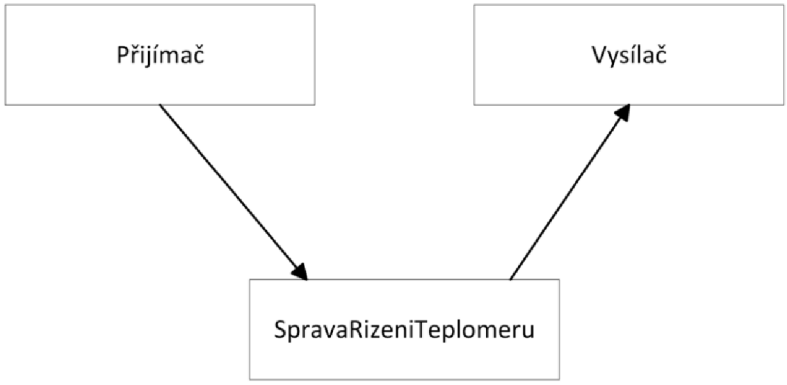
Aby bylo dosaženo nezávislosti a případné možnosti úpravy jednotlivých prvků systému bez narušení dat modelu, byla vybrána vrstevnatá architektura. Ta umožní uspořádání funkcí systému do jednotlivých vrstev. Každá vrstva využívá funkce a služby nabízené vrstvou umístěnou pod ní, a dále může poskytovat redundantní služby zajišťující tak vyšší spolehlivost celého systému. Pro potřeby tohoto návrhu byla zvolena čtyřvrstvá architektura.

Obr. 6.2 Návrh vrstevnaté architektury

Zdroj: vlastní zpracování.

6.7.3 Architektura systému shromažďování dat

Vzhledem k tomu, že specifická část dat popsaná v této práci výše jako objektová třída TeplomerPreprava shromažďuje informace o naměřené teplotě při logistickém procesu, je potřeba zajistit kontinuální přenos pomocí centrální jednotky online z přepravy do systému farmaceutické společnosti, který tato data dále ukládá do blockchain sítě. Proto je důležité vytvořit také architekturu tohoto systému zajišťující data. Níže je uveden jednoduchý návrh architektury pro shromažďování dat:



Obr. 6.3 Návrh architektury shromažďování dat pro teplotu v přepravě

Zdroj: vlastní zpracování.

6.8 Návrh řešení s využitím ElA Blockchain

Na jedné straně máme blockchain jako takový. Například Hyperledger od společnosti IBM, který nám poskytne dostačující informace o pravosti a kvalitě vakcíny. Avšak nikde se nehovoří o procesech, které vznikají od její výroby až po finální uskladnění, kde začíná její logistický proces. K tomu právě využijeme ElA blockchain, který byl již představen v této práci. Jeho možnosti jsou velice obsáhlé, ale nám postačí pouze pro ověření vydaných výrobních a logistických procesů.

Uvažujme tedy takto. Každá farmaceutická společnost, která vyrábí vakcíny a další medikamenty, musí postupovat podle předem stanovených legislativních, technologických a závazných norem a vyhlášek. Aby však procesy byly v souladu s nařízeními, je potřeba je implementovat, zavést do všech procesů a formalizovat formou dokumentace. Tato dokumentace je pravidelně revidována a vydávána jako závazný dokument směrem k odběratelům, kterými jsou očkovací centra. Aby však takto závazný dokument měl svou váhu a byl důvěryhodný, nestačí jej pouze distribuovat standardní cestou. Následky porušení těchto zásad může mít legislativní dopady, a proto farmaceutické společnosti provedou registraci do ElA blockchainu. Posléze tedy může veškeré tyto formalizované a schválené procesní dokumenty opatřit hashem, které vloží do ElA blockchain prostřednictvím aplikace Blockchain Notarius. Na závěr je možné provést distribuci formalizovaných výrobních procesů a sdílet je s očkovacími centry a týmy pro ověření kvality, kde každý dokument ponese svůj nezaměnitelný hash. Očkovací centra zapojená do ElA blockchainu si mohou posléze ověřit, zdali disponují

aktuální verzí za pomocí zadání hashe. V případě shody dojde k potvrzení prostřednictvím ElA blockchainu.

6.8.1 Propojení subjektů prostřednictvím Blockchain Notarius

Aby bylo možné toto řešení plně využívat, je potřeba provést registraci právnických subjektů do Blockchain Notarius. Zde jde o triviální záležitost, nicméně tuto registraci musí realizovat všechny zúčastněné strany bez ohledu na skutečnost, zdali budou v systému pouze číst, či zapisovat.

Klíčovou úlohu hrají farmaceutické společnosti, které budou aktivně hashovat dokumenty za pomocí této sítě a nástroje Blockchain Notarius.

7 Vyhodnocení vlastního návrhu

Zmíněné navržené řešení je ideálním využitím ve farmaceutickém průmyslu, neboť podléhá striktní kontrole ze strany regulátorů a vládních agentur. V tomto návrhu se podařilo posunout využití blockchainu na novou úroveň, a to skloubit standardní permissioned blockchain síť, vystavenou na produktu Hyperledger od společnosti IBM, pro záznam a sledování klíčových parametrů každé vyrobené vakcíny, které budou sloužit pro ověření pravosti a kvality každého vyrobeného balení, tak i ověření výrobních procesů konkrétní farmaceutické společnosti za využití ElA blockchain řešení, které naopak nebude poskytovat data, ale pouze bude sloužit pro ověření aktuálních publikovaných závazných technologických procesů napříč celým výrobním cyklem. Každá vládní organizace a očkovací centrum registrované do ElA blockchain si tak může ověřit přijaté dokumenty, konkrétně shodu hashe prostřednictvím ElA blockchainu.

Na tomto vystaveném základě se podařilo navrhnout řešení, které zamezí vakcinaci za pomoci nekvalitní či padělané očkovací látky a zároveň zajištění přístupu k procesní dokumentaci farmaceutické společnosti, která bude ověřitelná a platná vzhledem k povaze její závaznosti.

Závěr

Cílem této práce bylo navrhnout vlastní řešení využití technologie blockchain a ElA Blockchain ve farmaceutickém průmyslu. Návrhu pro demonstrování využití nesloužila žádná konkrétní farmaceutická společnost, nýbrž pouze zaměření se na daný sektor. Využití prostředků, které technologie blockchain a její aplikace nabízí, poskytuje možnost zvýšit důvěryhodnost, transparentnost a kvalitu vyrobených vakcín a zároveň tak uplatnit záznamy z logistického procesu pro sledování jejich pohybu. Uvedená technologie by mimo jiné umožnila zaručit věrohodnost distribuované dokumentace mezi očkovací centra a vládní instituce, která je závazná a popisuje výrobní a logistické procesy uvnitř konkrétní farmaceutické společnosti.

Velkou předností blockchainu je jeho možnost nasazení prakticky do jakéhokoliv odvětví, dalším benefitem je jeho využití. Je vhodné stanovit, pro jaké procesy a postupy se bude používat, jaké hodnoty bude zaznamenávat. Tato data mají nesmírnou cenu a stávají se součástí know-how, neboť je možné je využít jako podklad pro analýzy a predikce. Vzhledem k vysokému zabezpečení je blockchain ideálním řešením i tam, kde je bezpečnost dat, jejich integrita, dostupnost a věrohodnost na prvním místě. Obzvlášť v době masivní digitalizace, ke které došlo také vlivem pandemie SARS-COVID-2019. V dnešní době, kdy lze dokumenty podepisovat elektronicky a ověřovat na základě blockchainu, není již nezbytné držet vše pouze v papírové formě. Je tedy skutečností, že pandemie tomu velice napomohla a otevřela možnosti blockchainu i tam, kde by jen nad tím stěží top managementy společností uvažovaly. Bude velice zajímavé sledovat vývoj digitálního světa, využití blockchainu a ElA Blockchainu napříč podnikatelským spektrem. Navrhované řešení a jeho koncept je samozřejmě přenositelný na jiné podobné projekty.

Seznam zdrojů

[1] ANDERBERG, A., ANDONOVA, E., BELLIA, M., et al. *Blockchain now and tomorrow: assessing multidimensional impacts of distributed ledger technologies* [online]. Publications Office, 2019 [cit. 2021-06-15]. EUR (Luxembourg. Online). ISBN 9789276089773. Dostupné z: https://publications.jrc.ec.europa.eu/repository/handle/JRC117255.

[2] SHOBHIT, S. *Public, Private, Permissioned Blockchains Compared*. Investopedia: Sharper insight, better investing. [online]. 29. 6. 2021. [cit. 2021-07-11]. Dostupné z: https://www.investopedia.com/news/public-private-permissioned-blockchains-compared/.

[3] LEE, David a Robert DENG, ed. *Handbook of blockchain, digital finance, and inclusion*. London: Academic Press, [2018]. ISBN 978-0-12-810441-5.

[4] DRESCHER, Daniel. *Blokchain basics: a non-technical introduction in 25 steps*. [Berkeley, California]: Apress, [2017]. ISBN 978-1-4842-2603-2.

[5] A11. *Man in the Middle – MITM*. NášRegion.cz [online]. A11 s.r.o., Copyright © 2015-2021, 19. 1. 2021 [cit. 2021-08-13]. Dostupné z: https://nasregion.cz/praha/man-in-the-middle-mitm/.

[6] MICROSOFT CORPORATION. *SHA512 třída*. Microsoft.com [online]. Microsoft, Copyright © Microsoft 2021, [cit. 2021-08-13]. Dostupné z: https://docs.microsoft.com/cs-cz/dotnet/api/system.security.cryptography.sha512?view=net-5.0.

[7] JOHNSON, D., MENEZES, A. a S. VANSTONE. The Elliptic Curve Digital Signature Algorithm (ECDSA). *International Journal of Information Security* [online]. 2001, **1**(1), 36-63 [cit. 2021-8-13]. ISSN 1615-5262. Dostupné z: https://link.springer.com/article/10.1007/s102070100002.

[8] NASR, S. *Hard Forks vs. Soft Forks (and how they work with Blockchain)*. LinkedIn.com [online]. LinkedIn, Copyright © 2021, 26. 6. 2019 [cit. 2021-08-13]. Dostupné z: https://www.linkedin.com/pulse/hard-forks-vs-soft-how-work-blockchain-salah-nasr?articleId=6549493038530555904.

[9] DHL CUSTOMER SOLUTIONS & INNOVATION. *Blockchain in Logistics*. Dhl.com [online]. DHL International GmbH, Copyright © 2021, 2018. [cit. 2021-08-11]. Dostupné z: https://www.dhl.com/content/dam/dhl/global/core/documents/pdf/glo-core-blockchain-trend-report.pdf.

[10] ELA BLOCKCHAIN SERVICES. *ElA blockchain je blockchain pro váš business: Informace o ElA blockchainu a možnostech jeho využití.* Electroindustry.cz [online]. ELA Blockchain Services a.s., Copyright © 2021. [cit. 2021-08-13]. Dostupné z: https://www.electroindustry.cz/fs/e1421171-4680-11ea-aac5-00155d092b8f-blockchain-brozura-cz.pdf.

[11] SOMMERVILLE, I. *Softwarové inženýrství*. Brno: Computer Press, 2013. ISBN 978-80-251-3826-7.

Seznam grafických objektů

Seznam obrázků

Seznam tabulek

Autor/ka	**Jason Parker Kubik, DiS.**
Název BP	**Technologie Blockchain v logistice**
Studijní obor	**IPL**
Rok obhajoby BP	**2021**
Počet stran	45
Počet příloh	0
Vedoucí DP	**prof. Mgr. Roman Jašek, Ph.D., DBA**
Anotace	Bakalářská práce je zaměřena na využití technologie blockchain ve farmaceutickém průmyslu s ohledem na její logistické procesy při výrobě a distribuci vakcín a ověřování výrobních a logistických procesů formou využití ElA Blockchainu. V teoretické části je popsáno fungování blockchainu z pohledu bezpečnosti, architektury, využití frameworků, ale také jeho vývojové etapy a využití v logistice a dalších odvětvích. Praktická část představuje návrh využití blockchainu a ElA Blockchainu ve farmaceutickém průmyslu. Tato práce také vyhodnocuje přínosy návrhu pro konkrétní odvětví.
Klíčová slova	Blockchain, hash, IT bezpečnost, farmaceutický průmysl, ElA Blockchain, Blockchain Notarius
Místo uložení	ITC (knihovna) Vysoké školy logistiky v Přerově
Signatura	