ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ

FAKULTA DOPRAVNÍ

MATÚŠ DANIEL

BLOCKCHAIN V LETECTVÍ

DIPLOMOVÁ PRÁCE

ROK ODEVZDÁNÍ DIPLOMOVÉ PRÁCE

2020

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
Fakulta dopravní
děkan
Konviktská 20, 110 00 Praha 1

K621 .....**Ústav letecké dopravy**

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení studenta (včetně titulů):

Bc. Matúš Daniel

Kód studijního programu a studijní obor studenta:

N 3710 – PL – Provoz a řízení letecké dopravy

Název tématu (česky): **Blockchain v letectví**

Název tématu (anglicky): Blockchain in Aviation

Zásady pro vypracování

Při zpracování diplomové práce se řiďte následujícími pokyny:

- Úvod do technologie Blockchain
- Blockchain v obchodní letecké dopravě
- Blockchain v soukromé letecké dopravě
- Blockchain pro účely údržby a servisu letadel
- Blockchain pro letecký personál
- Blockchain jako měna

Rozsah grafických prací: dle pokynů vedoucího diplomové práce

Rozsah průvodní zprávy: minimálně 55 stran textu (včetně obrázků, grafů a tabulek, které jsou součástí průvodní zprávy)

Seznam odborné literatury: Bitcoin and Cryptocurrency Technologies: A comprehensive Introduction Hardcover (July 19, 2016 Od autorů Arvind Narayanan , Joseph Bonneau, Edward Felten, Andrew Miller, ISBN-13: 978-0691171692)

Blockchain Revolution (Don Tapscott, ISBN:978-0-241-23785-4)

Vedoucí diplomové práce: **Ing. Ladislav Capoušek, Ph.D.**

Ing. Ota Hajzler

Datum zadání diplomové práce: **27. července 2018**
(datum prvního zadání této práce, které musí být nejpozději 10 měsíců před datem prvního předpokládaného odevzdání této práce vyplývajícího ze standardní doby studia)

Datum odevzdání diplomové práce: **18. května 2020**
a) datum prvního předpokládaného odevzdání práce vyplývající ze standardní doby studia a z doporučeného časového plánu studia
b) v případě odkladu odevzdání práce následující datum odevzdání práce vyplývající z doporučeného časového plánu studia

L. S.

doc. Ing. Jakub Kraus, Ph.D.
vedoucí
Ústavu letecké dopravy

doc. Ing. Pavel Hrubeš, Ph.D.
děkan fakulty

Potvrzuji převzetí zadání diplomové práce.

Bc. Matúš Daniel
jméno a podpis studenta

V Praze dne 10. února 2019

Poděkování

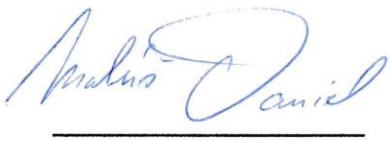
Rád bych zde poděkoval všem, jejichž rady mi byly nápomocny při tvorbě diplomové práce, zvláště pak Ing. Otovi Hajzlerovi a Ing. Ladislavovi Capouškovi, Ph. D., za cenné rady a odborné vedení práce. Dále bych chtěl poděkovat svým rodičům a všem blízkým, kteří mě podporovali nejenom při tvorbě této práce, ale po celou dobu mého studia.

Čestné prohlášení

Prohlašuji, že jsem tuto písemnou práce vypracoval samostatně, pouze za odborného vedení obou vedoucích diplomové práce.

Dále prohlašuji, že veškeré podklady a zdroje, ze kterých jsem čerpal, jsou uvedeny v seznamu použité literatury v souladu s Metodickým pokynem o etické přípravě vysokoškolských závěrečných prací. Nemám závažný důvod proti užívání tohoto školního díla ve smyslu § 60 Zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

V Praze, dne 12. 5. 2020



Matúš Daniel

Abstrakt

Diplomová práce představuje technologii blockchain a s tím spojenou tvorbu decentralizovaných sítí. Inovativní způsob torby digitální infrastruktury bude v budoucích letech nacházet stále více využití napříč letecké obory. Práce se zaměřuje jak na seznámení se základními pojmy, tak zpracovává možnosti implementace v odvětví leteckého průmyslu. Dále vysvětluje jaké jsou její finanční a konceptuální výhody. Práce nezaměřuje pouze na jedinou aplikaci, ale zpracovává spektrum možných využití v letectví. Autora především zajímají otázky využití blockchainu v oblasti elektronické identity, zjednodušení procesů a zvýšení důvěryhodnosti digitálních dat.

Klíčová slova

blockchain, digitální, infrastruktura, identita, data, osobní doklady, letectví, sítě, zápisník, letů

Abstract

Master´s thesis intends to introduce new technology, which in upcoming years will spread in vast majority of industries where it might change ways of storage and sharing of the digital data. Blockchain, as an innovative architecture will most probably influence aviation industry as well and aspire to bring answers to some of the technological challenges of nowadays. Thesis is focusing on explanation of basic concepts and blockchain implementation in civil aviation. Attention is given to creation of digital identity and digital data for aircraft manufacture and maintenance. Explanations throughout the chapters are supported by visualizations and schemes of communication channels and its nodes. Final part of the thesis focuses on financing and starting projects in university environments, where it can support general knowledge and further understanding of blockchain technology.

Key words

blockchain, digital, infrastructure, identity, data, documents, aviation, network, logbook

Obsah

1 Seznam použitých zkratek

ADS-B	Automatic Dependent Surveillance – Broadcast
App	Aplikace
BFT	Tolerance Byzantské chyby (Byzantine Fault Tolerance)
COVID-19	COrona VIrus Disease- 2019
CPU	Procesor (Central Processing Unit)
dApp	Decentralizovaná aplikace
DDOS	Distributed Denial Of Service
DID	Decentralizovaný Identifikátor (Decentralised Identifier)
DOS	Denial Of Service
DOT	Token sítě Polkadot
DPKI	Decentralized Public Key Infrastructure
DPoS	Delegovaný Důkaz vlastnictvím (Delegated Proof of Stake)
EAA	Ethereum Enterprise Alliance
FAA	Federální letecká správa (Federal Aviation Administration)
IATA	Mezinárodní asociace leteckých dopravců (International Air Transport Association)
ICAO	Mezinárodní organizace pro civilní letectví (International Civil Aviation Organization)
ICO	Initial Coin Offering
IEO	Initial Exchange Offering
IoT	Internet věcí (Internet Of Things)
ISS	Vypořádací systémy IATA (IATA Settlement Systems)
KYC	Poznej svého klienta (Know Your Custommer)
MRO	Provoz a údržba (Maintenace, Repair and Overhaul)
NONCE	Číslo použité pouze jednou (Number used Only Once)

P2P	Peer to Peer
PKI	Public Key Infrastructure
PoET	Důkaz uplynulého času (Proof of Elapsed Time)
PoS	Důkaz vlastnictvím (Proof of Stake)
PoW	Důkaz prací (Proof of Work)
SAFA	Safety Assesment of Foreign Aircraft
SGX	Software Guard Extension
SRA	Safety Restricted Area
STO	Security Token Offering
TEE	Trusted Execution Environment

2 Úvod

Žijeme ve velice dynamickém čase, kdy je nutné se čím dál rychleji adaptovat novým trendům. O to více to platí pro letectví, které vždy šlo příkladem v adopci nových standardů. Jedním z inovativních trendů je dle studie "*Future of the Airline Industry 2035*" i technologie blockchain. [1]

Návrhy databáze zabezpečené kryptografickými procesy vznikaly již během devadesátých let dvacátého století. První reálné aplikace technologie blockchain se však svět dočkal až do roku 2008. Jedinec, nebo skupina pod pseudonymem Satoshi Nakamoto vytvořila první decentralizovanou distribuovanou databázi. Databáze plní funkci účetní knihy. Jsou do ní zapisovány transakce, které jsou sítí automaticky kontrolovány, potvrzovány a ukládány jako bloky dat. Bloky jsou pomocí kryptografických procesů v pevném pořadí vázány jeden k druhému. Měna, se kterou účetní kniha pracuje se nazývá Bitcoin. Hodnota Bitcoinu je podložena vynaloženou energií, která je do systému investována. Odborníci nazývají vytvoření standardu a spuštění Bitcoinu etapou Blockchain 1.0. Následující etapa (Blockchain 2.0) vývoje začala v roce 2015, kdy byla spuštěna další distribuovaná databáze na základě nové kryptoměny. Jednalo se o kryptoměnu Ethereum. Ethereum vytvořil efektivnější a rychlejší prostředí, než umožňuje Bitcoin. Ethereum nabídl světu možnost vytvářet decentralizované aplikace v různých programovacích jazycích, které mohou využívat rozsáhlou uživatelskou síť a její potenciál. Největším přínosem etapy Blockchainu 2.0 je možnost implementace Smart kontraktu a přidání možnosti zapisovat do bloků data jakéhokoliv charakteru. Zmíněný Smart kontrakt umožňuje uzavírat a plnit smlouvy, nebo transakce, bez nutnosti prostředníka, jakým jsou například banky. Nejen, že je tak možné se zbavit výdajů za brokerské služby, ale také umožňuje se zbavit závislosti na lidském faktoru, pracovních dnech, hodinách, nebo na stabilitě firmy a trhu. Obousměrné plnění kontraktu probíhá nezávisle, legálně, bezpečně a okamžitě za pomoci matematických procesů. Současná etapa vývoje blockchainu je na pomezí druhé a třetí etapy vývoje. Třetí etapa má zajistit implementaci blockchainových technologií do vhodných odvětví průmyslu, medicíny a státní správy. Zapojením stále dokonalejší sítě IoT (Internet Of Things), 3D tiskáren, umělé inteligence a umělé intuice, může blockchain pomoci skrz společnost zvýšit důvěru, bezpečnost a stabilitu. Odborníci napříč obory začali vytvářet dokumenty s názvem „White paper". Autoři dokumentů se zamýšlí nad možnostmi implementace, výhodami a základní problematikou spojenou s realizací projektů využívající decentralizované databáze. Jedním z takových

dokumentů má být tato diplomová práce. Její struktura je koncipována tak, aby sloužila jako základ pro další projekty propojující blockchain a civilní letectví. V každé kapitole se mísí praktická i teoretická část, tak aby čtenáři práce přinesla co nejširší pochopení problematiky. Práce se zaměřuje na tvorbu digitální infrastruktury v letectví, kde zabezpečená elektronická komunikace pomůže používání digitální identity jak pro personál, cestující, tak následně i pro letouny a jejich díly.

Blockchain je tím důvěryhodnější a transparentnější systém, čím více subjektů se na síti podílí. Proto nachází využití v oborech, kde spolu blízce spolupracuje velké množství poskytovatelů služeb. Letectví bezpochyby jedním z takových oborů je. Letouny jsou složené z miliónů částí, od stovek různých dodavatelů. Následně jsou prodávány leteckým společnostem, které jsou spojené pod aliancemi a organizacemi. Létají na desetitisíce letišť, ležících ve více než dvou stech zemích světa. Obsluhovány jsou posádkami různých národností, mající rozdílné kvalifikace, zkušenosti a výcvik. Chyba, zanedbání, nebo zaváhání jednoho z mnoha subjektů podílejících se na letecké dopravě, může mít fatální důsledky pro celý průmysl. Jedním výstražným příkladem, který stále ovlivňuje trh, je zanedbaný vývoj letounu Boeing 737 MAX. Kvůli nedotaženému, netransparentnímu vývoji a nedostatečné kontrole ze strany FAA, přišly o život stovky cestujících. Zároveň se však destabilizoval celý letecký průmysl. Letecké společnosti byly nuceny řešit nečekané logistické problémy a měnit rozvojové plány do budoucna. Tisíce zaměstnanců o práci přišlo a další desetitisíce se strachují, že krize ovlivní i jejich pracovní pozice. [2]

Počet přepravených cestujících od roku 1970 (cca 310 mil. Cestujících) do roku 2017 (cca 4 233 mil. Cestujících) se přibližně třináctkrát zvýšil. Nárůst počtu přepravených osob, bylo možné zvládnou pomocí investice do zásadních inovací , které pomáhaly měnit tvář moderního světa. První zásadní revolucí bylo využívání výpočetní technologie v letectví. Na přelomu sedmdesátých a osmdesátých let se výpočetní technologie začala šířit do všech myslitelných odvětví. Výpočetní technologie zásadně ovlivnila strukturu a práci s ukládanými daty. Mnoho procesů bylo možné přesunout z analogické formy do digitální formy. Digitální podstata procesů pomohla zaznamenávat mnohem více dat, dělat přesnější statistiky a dynamicky reagovat na vývoj na trhu. Pomohla řídit letadla, vývoj a firmy přesněji a účinněji. Odborníci potenciál využili a začali investovat do tvorby programů, které personálu ulehčily práci a skokově snížily chybovost lidského faktoru. Poprvé v historii tak bylo možné jednoduše vyhodnocovat obrovská kvanta dat s naprostou přesností. Dalším milníkem, který umožnil exponenciální růst leteckého průmyslu, byl příchod internetu. Internet propojil v reálném čase celý svět. Začalo se pracovat

s Velkými daty (Big Data), která následně pomáhají řešit bezpečnostní, ekologické a ekonomické výzvy. Internet dal vzniknout konceptu Globálního distribučního systému letenek zajišťují efektivnější prodej letenek, marketingu a zkoumání chování zákazníků (KYC – Know Your Custommer). Cestující mohou nakupovat letenky , spravovat rezervace a dokončit odbavení v reálném čase a v pohodlí domova. Vytvoření globální sítě však přineslo mnoho dalších výhod, bez kterých se moderní letecký průmysl již nemůže obejít. [3] [4]

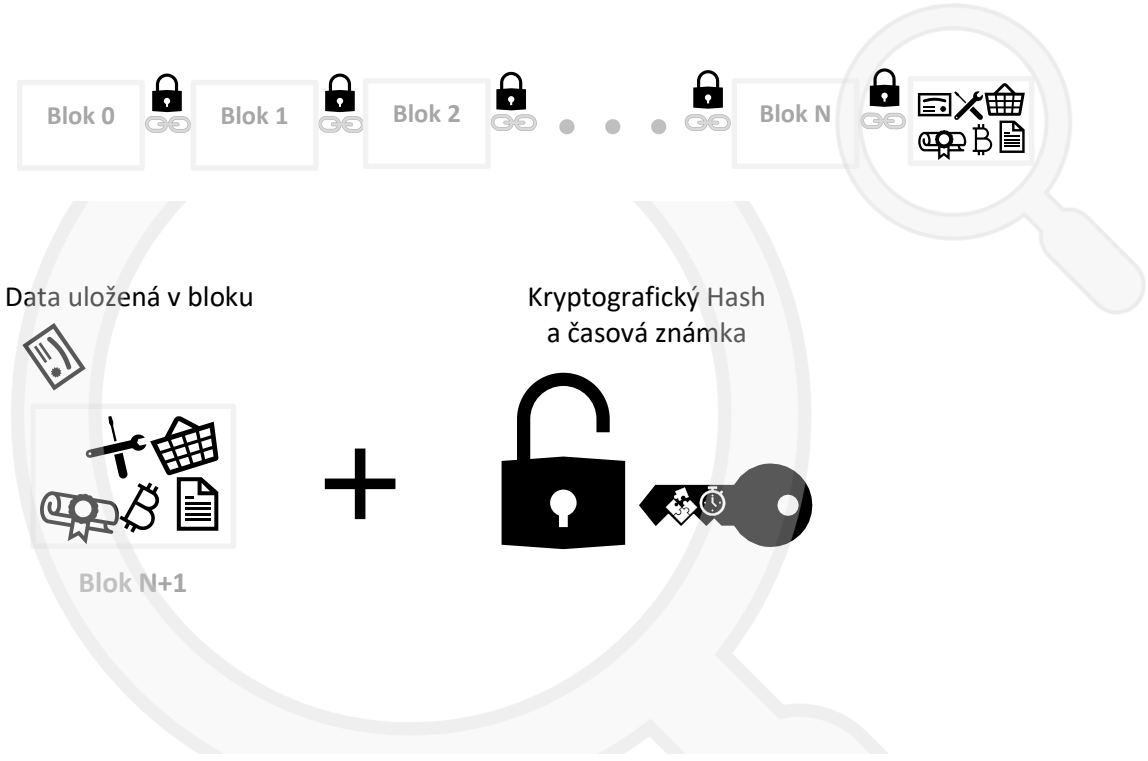
Studie firmy Boeing („*Commercial Market Outlook 2019 – 2038*“) však ukazuje, že předpokládaný počet komerčně provozovaných proudových letounů se do roku 2038 má až zdvojnásobit. Proto přichází čas přemýšlet, jak bude možné tuto komplexní letku efektivně a bezpečně provozovat. Jedním ze základních problémů výpočetní technologie a internetu je nedostatečná důvěryhodnost. Proto je klíčové vytvořit sítě, ve který budou všechna data důvěryhodná, zdroje informací dohledatelné a nenapadnutelné. Blockchain nabízí tvorbu globálních decentralizovaných sítí, kde jsou si všichni účastníci sítě rovni. Sítě jsou zabezpečené svou matematickou podstatou. Kontrola není prováděna centrálním subjektem, popřípadě subjekty, ale je konána všemi uživateli sítě zároveň. Díky blockchainu je možné propojit transparentní dodavatelské řetězce s internetem věcí, kde každá součástka bude moci být kontrolována, objednávána, nebo opravována automaticky a v reálném čase. Automatizace pomůže nedostatku kvalifikované pracovní síly napříč leteckým průmyslem. Personální kapacity tak budou moci být využívány pro stabilizaci a rozvoj průmyslu. Zároveň ekonomický ekosystém se může zbavit poplatků třetím stranám, bankám a státům, což při správných rozhodnutích povede k efektivnějšímu financování udržitelného rozvoje. Pokud má ke zdvojnásobení počtu cestujících dojít, musíme zvýšit propustnost letišť, bez toho abychom ohrozili bezpečnost povozu. Propustnost letiště závisí z velké části na propustnosti bezpečnostních kontrol. Proto je nutné jednotlivé stanoviště prohlídek spojit a zefektivnit. Blockchain může napomoci tvorbě elektronické identity, která by nahradila nutnost fyzické podoby letenky a osobních dokladů. Čtečka by pomocí jedinečného otisku obličeje, či prstů rozpoznala identitu cestujících a s ní spojenou palubní vstupenku. Na základě tohoto skenu pak systém automaticky vyhodnotí povolení, či zamítnutí přístupu do SRA.

S digitalizací osobních dokladů, je také nutné aktualizovat podobu dokladů pro identifikaci posádek. Vhodné je proto zároveň přistoupit k vytvoření elektronické podoby leteckých způsobilostí posádek a jinak certifikovaného personálu. Letecké úřady by mohly poprvé v historii vytvořit globální databázi leteckého personálu a posílit tak důvěryhodnost napříč leteckým průmyslem a současně cestujícími. Autority tímto získají nástroj pro efektivní kontrolu. Budou moci

lépe vyhodnocovat dobu služby posádek, nebo nutnost prodloužení kvalifikací. Pokud se podaří systémy rozšířit celosvětově, bude civilního letectví o krok blíže ke globálnímu sjednocení legislativy. Zjednodušení zároveň přinese mnoho výhod i aerolinkám. Získají přístup k důvěryhodným informacím o pilotech, zákaznících, nebo o chování trhu. Velká data, by následně za pomoci umělé inteligence a intuice, mohla pomoci s predikcí a potlačením hrozeb. Blockchain dále nabízí cílené a selektivní sdílení dat, které pomůže uživatelům chránit svoji identitu, firmám se vyhnout sankcím za porušení pravidel ochrany osobních dat, GDPR. Reálná aplikace kryptoměn jako oficiálního platidla by mohla pomoci nastavit celosvětové věrnostní programy, které budou podloženy reálnou hodnotou.

3 Úvod do technologie Blockchain

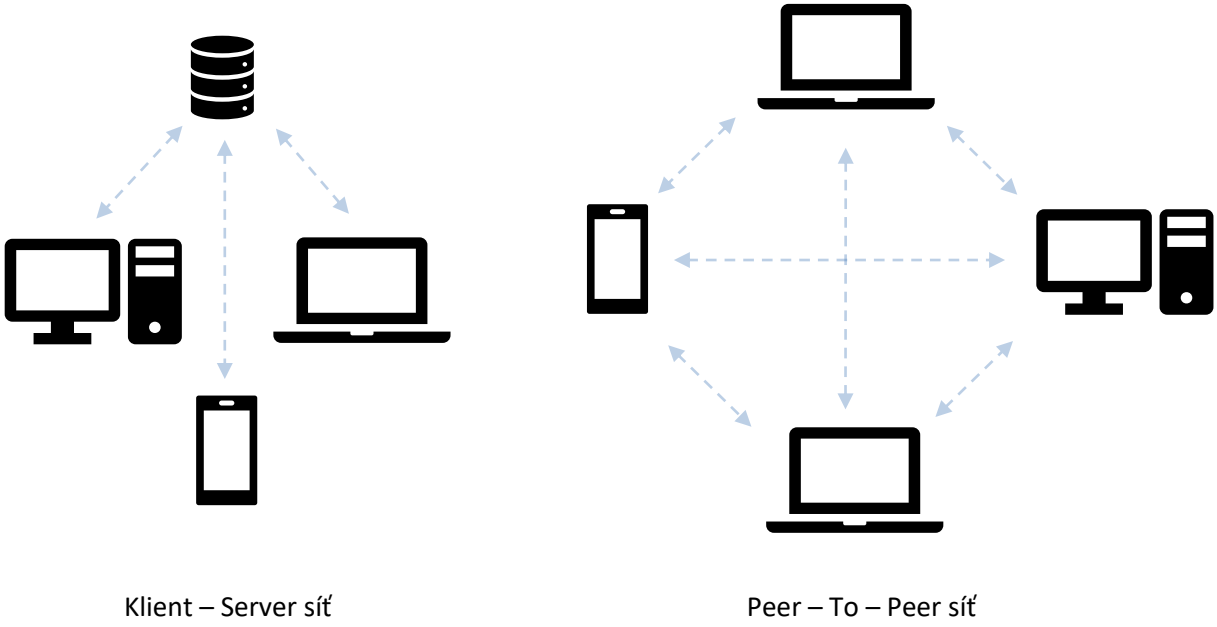
Blockchain, česky Bločenka je databáze, která umožňuje uchovávat a zároveň sdílet data v rámci uživatelských decentralizovaných sítí. Data jsou ukládána do přesně definovaných bloků vázaných za sebe, do formy řetězce. První blok celého řetězce se v anglické terminologii nazývá „Genesis Block“, nebo jinak Blok 0. Blok 0 je vytvořen tvůrcem sítě, všechny následující bloky jsou již vytvářeny a kontrolovány za pomoci účastníků sítě. Jakmile je nový blok naplněný informacemi je připojen k řetězci a pomocí kryptografické pečetě uzavřen. Kryptografická pečeť se v Blockchainové terminologii nazývá Hash. Spolu s časovou známkou vytváří bezpečnostní prvek, zabezpečující přesné a nezměnitelné pořadí v bloků v Blockchainu. Celý blok tak po uzavření obsahuje nový Hash, Hash předešlého bloku a čas, kdy byly informace do bloku zapsány. Závislost bloků mezi sebou, nám zajišťuje, že informace na sebe přímo navazují a není možné předešlé bloky nahrazovat, nebo dokonce vkládat do řetězce nové, či falešné bloky. Zajištění vysoké integrity, bezpečnosti, důvěryhodnosti a transparentnosti, nám v budoucnu pomůže zefektivnit ochranu osobních údajů, nebo vlastnického práva.



Obrázek 1 Přiřazení bloku do řetězce

Samotná architektura databáze se nazývá peer-to-peer. Drtivá většina dnešních databází, i samotné fungování internetu (Wolrd Wide Web) je založeno na centrální serveru (databázi, nebo více databázích), který oprávněným uživatelům dovolí prohlížet uložené soubory. Server uchovává všechna data na jednom místě, kde je skupina administrátorů kontroluje, udržuje a aktualizuje. Takovéto systémy jsou plně centralizované. [5]

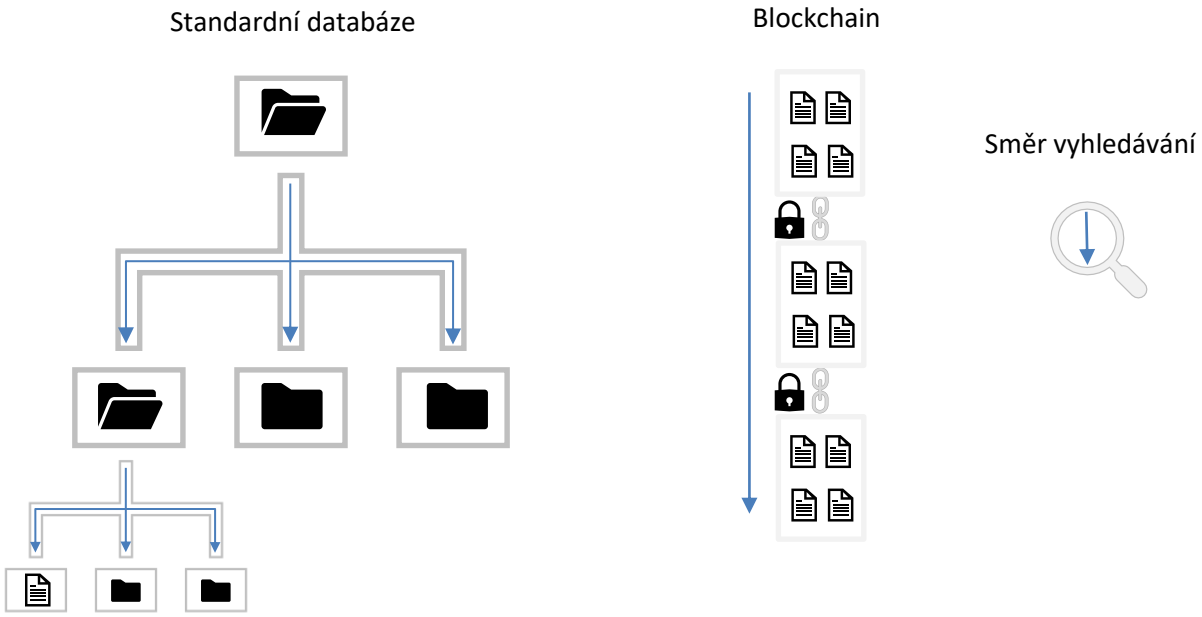
Peer-to-peer (P2P) architektura nabízí demokratický pohled na stavbu sítí. Uživatelé využívající síť, se musí o bezpečnost a funkčnost sítě starat sami. Neexistuje centrální autorita a všichni uživatelé sítě jsou si mezi sebou rovni. Základní výhodou oproti Klient – server architektuře je nezávislost na jednom centrálním serveru. Pokud je server v architektuře Klient- Server odpojen, celá síť přestane plnit svoji funkci. Na rozdíl od konceptu Klient – Server je P2P síť aktivní do té doby, dokud jsou aktivní její uživatelé. [5]



Obrázek 2 Porovnání server-uživatel a peer-to-peer architektury [5]

Blockchain je tedy distribuovaná decentralizovaná databáze v rámci peer-to-peer sítě. Její hlavní výhody jsou snížení nákladů na provoz sítě, efektivnější vyhledání, zvýšení bezpečnosti a důvěryhodnosti dat. Snížení nákladů je způsobeno velkou soběstačností sítě a bezpečností vycházející, ze samotného konceptu, kde se síť uživatelů v kontrole zabezpečení angažuje. Další výhodou oproti jiným databázím je velmi efektivní způsob vyhledávání. To je ze dvou základních důvodů. V blockchainu je možné vyhledávat pouze v jednom směru. Všehna data jsou uložena v linii za sebou, na rozdíl od centralizovaných databázích se ukládají informace do stromu složek a souborů. Druhým důvodem je přímá závislost všech bloků v řetězci. Každý

předšlý blok řetězce, je díky funkci Hash součástí dalšího bloku. V standartních databázích na sobě ukládaná data nemají návaznost. [5]



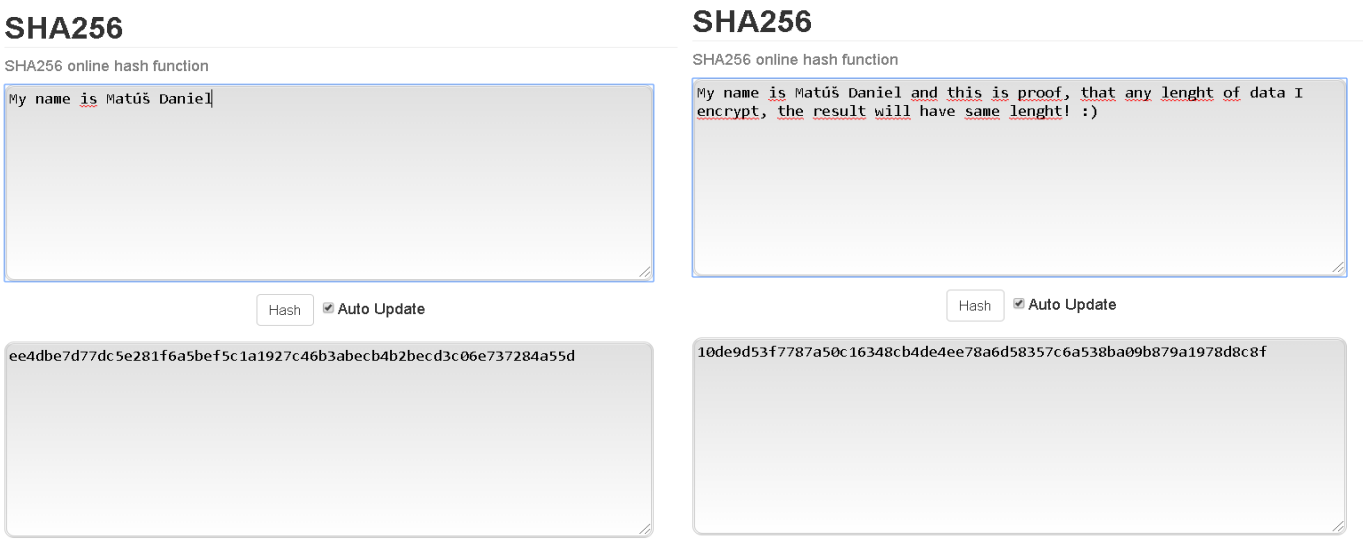
Obrázek 3 Znázornění vyhledávání ve standardní a blockchainové databázi[Autor]

Okolo blockchainu je možné vytvářet aplikace, které využívají data, nebo měny pohánějící síť. Tyto aplikace se nazývají decentralizované aplikace, zkráceně dApps. Standardními aplikacemi tohoto typu jsou aplikace Wallet. Aplikace Wallet dávají přístup k informacím jednotlivých uživatel. Zároveň se ale se může jednat o aplikace obchodníků, úřadů, nebo firem, které v rámci sítí operují. Může se jednat o aplikace ve formě internetových obchodů, nebo například archivů dat.Základním rozdílem mezi klasickými aplikace a decentralizovanými aplikacemi je nezávislost na jednom centrálním serveru. Fungují v rámci uživatelské sítě vyboduvané kolem blockchainu. Uživatelé musí, pro práci s aplikacemi, být připojeni k síti, kde za použití Smart kontraktů mohou pracovat s daty a tokeny, které jsou do blockchainu pod hlavičkou jejich privátního klíče uloženy. Stejně tak mohou za pomoci Smart kontraktů žádat o data a tokeny ostatních uživatel. Decentralizované aplikace mohou být sítí zpoplatněné jako je tomu u Ethernea, kde se platí za každou zapsanou informaci do řetězce. Nebo jsou zcela zadarmo, jako u většiny veřejných, hybridních i privátních blockchainů

3.1 Blok

Stavba bloku je v každém systému lehce odlišná. Záleží hlavně na konečném využití databáze- Vysvětlení principů je zde provedeno na příkladu nejjednoduššího, zároveň nejrozšířenějšího

blockchainu, kterým je Bitcoin. Základní premisa je však vždy stejná. Bloky obsahují informace v přesném pořadí a s jasným zdrojem. V Bitcoinu návaznost zaručuje kombinace základních prvků. Základními prvky blockchainu je časová známka, verze blockchainu (v tomto případě verze Bitcoinu), kořen Merkle root, hash a obsahová část. Hash je základním kamenem procesu připojování bloků a tvorby celého blockchainu. Tato funkce vytváří při vložení dat jedinečný kód o konstantní délce. Délka kódu závisí na typu kódování, který si autor pro dané využití vybral. Spojování (hashování) dvou stejných souborů dat dohromady, vytvoří vždy stejný výsledný kód. Jako ochranný prvek slouží nevratnost této funkce. Jakmile jednou data zakódujeme, není možné zpětně zjistit s jakými daty program pracoval. Dalším bezpečnostním prvkem je konstantní délka výsledného kódu. Díky vždy stejné délce výsledku, není možné odvodit, s jak velkým souborem dat program pracoval. V blockchainových technologiích se používá Hashování k vytvoření originálního otisku informací, které vkládáme do řetězce. Jedná se o punc jedinečnosti, zabezpečující důvěryhodnost dat.[6]



Obrázek 4 Příklad kódu vytvořeného funkcí SHA256[8]

Verze bloku, popisuje, jaká je struktura dat v bloku a to podle zadání zřizovatele databáze. Je používána pro standardizaci a pro jednoduché čtení informací uvnitř bloku. Dále pomáhá zařízením fungovat v rámci nejaktuálnější verze.[6]

Hash kořene Merkle root je vytvořen slučováním (hashováním) jakýchkoliv dvou a více informací dohromady. Vytváří jejich unikátní otisk, který později zjednodušuje jejich podobu a umožňuje jednodušší vyhledávání. Při ověřování integrity dat se tak zbavíme nutnosti mít na každém zařízení celý blockchain, ale pracujeme pouze s hlavičkami bloků. Blok totiž může obsahovat i

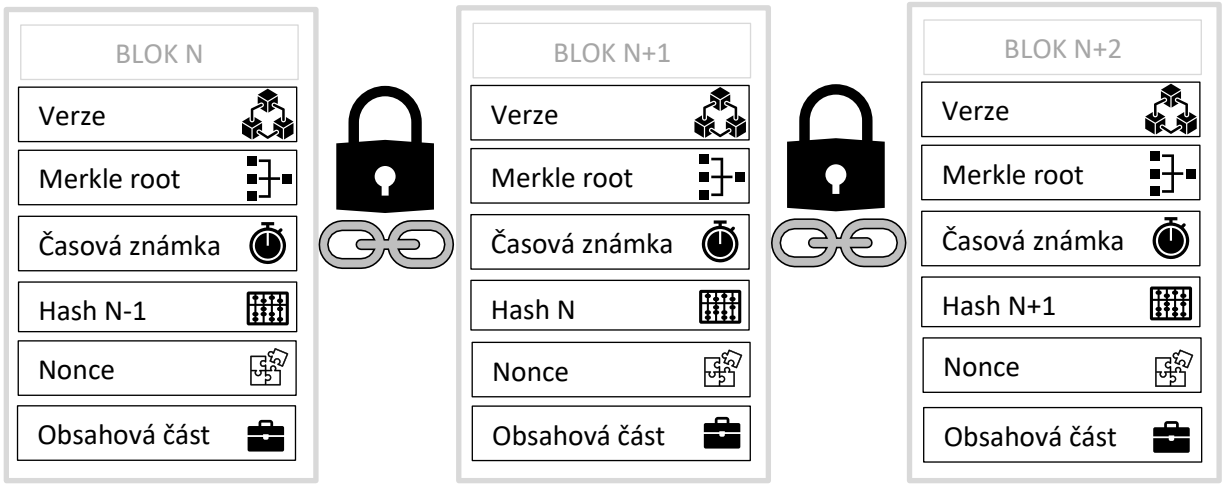
několik miliónů bytů. Využíváním zkrácené verze blockchainu je možné pro práci v rámci sítě snížit výměnu dat na pouhých desítek několik desítek bytů.[6]

Časová známka identifikuje, kdy byl blok vytvořen. Datuje se na uběhlý „Unix čas“. To znamená čas, který uplynul od 00:00 1.1.1970. [6]

Hash předešlého bloku je unikátní kód, který obsahuje každý blok. Tento kód nám oznamuje přesnou návaznost bloků za sebou.[6]

Nonce (Number Only Used Once) je pseudonáhodné číslo, nezbytné k vytvoření bloku. Používá se v systémech, kde je k uzavření bloku nutno vynaložit práci. Práce je vykonávána těžařem, jehož úkolem je vytvořit unikátní Hash odpovídající podmínkám pro uzavření bloku (například počet nul na začátku kódu). Těžařův počítač náhodně generuje čísla, která za pomoci kryptografické funkce kombinuje s otiskem předešlého bloku. Kombinací je vytvořen unikátní Hash, který následně porovnává s podmínkami pro uzavření bloku. Jakmile se těžaři podaří najít správnou kombinaci čísel, je možné blok uzavřít a distribuovat všem uživatelům. Těžař je následně za vynaloženou energii odměněn. [6]

Obsahová část obsahuje data, která jsou do blockchainu zapisována. V případě kryptoměn jsou to záznamy o transakcích tokenů. V Případě jiných průmyslových řešení to mohou být například data o stavu a lokaci určitého produktu. Jejich struktura odpovídá využití a stavbě sítě. Velikost obsahové části se také liší v závislosti na aplikaci. Pro představu u kryptoměny Bitcoin je to fixně 1mb. U Ethernea se v průměru se jedná o 20–30 kb. [6] [7]



Obrázek 5 Pořadí bloků v blockchainu [Autor]

4 Tokenizace

V první blockchainové síti (Bitcoin) jsou tokeny synonymem slova kryptoměna. Jedná se o virtuální jednotku, která představující určitou hodnotu. U Bitcoinu je tato hodnota podložená výpočetní silou, kterou uživatelé sítě vkládají do jejího provozu. Tento princip je společný pro většinu veřejných blockchainů, kde práce účastníků sítě je odměňována tokeny, které mají hodnotu vyčíslitelnou v reálné měně. Tokeny však, s novými koncepty využití blockchainových sítí, získávají různé podoby. V leteckém průmyslu mohou představovat hodnotu práce jednoho specialisty, hodnotu letenky, nebo poplatek za vykonání úředního úkonu, jako je vydání letecké licence, nebo správní poplatek za registraci letounu. Tokeny tak mohou vytvořit prostředí v rámci jednoho průmyslu, které mohou zajistit financování projektů, distribuci dotací a zároveň sloužit jako platební jednotka v případě reklamací letenek, nebo práci s věrnostními programy. Průmyslové prostředí tím získá nástroj k přímé a transparentní funkci bez nutnosti prostředníků jakými jsou banky, nebo platební portály. Zrušením prostředníků se tak získá zjednodušení a tím snížení cen procesů. Organizace IATA (International Air Transport Association) si tyto výhody uvědomila a začala vyvíjet svojí vlastní kryptoměnu. Jedním z hlavních prvků asociace jsou takzvané IATA Settlement Systems (ISS), tvořící páteřní systém globální ekonomiky leteckého průmyslu. Služby ISS zajišťují rychlý, bezpečný a efektivní způsob přesunu financí mezi aerolinkami, státy, výcvikovými centry, řízením letového provozu a dalšími důležitými zprostředkovateli leteckých služeb. Tento projekt zajistil v roce 2017 financí v hodnotě 433.3 miliard dolarů. [8]

Finanční transakce v leteckém odvětví představují ohromné částky. Ty se pohybují v mezinárodním prostředí a mezi různými subjekty a bankami. Takto je v procesu utráceno nezanedbatelné procento zdrojů, které by se jinak daly použít například na rozvoj leteckého průmyslu, zvýšení komfortu, či snížení cen za letenky. Proto se společnost IATA zaměřila na tvorbu vlastní kryptoměny IATA Coin. Jako důkaz správnosti tohoto konceptu přesunula IATA 1000 dolarů do čtyř společností ve čtyřech různých státech. Na konci cesty z peněz, které IATA poslala bylo ztraceno 20 % zdrojů v poplatcích za služby, které si poskytovatelé služeb vzájemně účtovali. IATA Coin již existuje v malém testovacím ekosystému, mezi několika prostředníky. Je podložena hodnotou peněz, takže je, prozatím, takzvanou měnou s nuceným oběhem. Je podložena americkými dolary, eury a anglickými librami. Aerolinky mohou tuto měnu nakupovat, za reálné peníze a v reálné hodnotě. Tímto je zabráněno její volatilitě. Pokud se organizaci IATA podaří vytvořit platformu pro blockchainovou síť, která bude podporována

všeobecně uznávanou měnou, bude možné vytvořit velmi efektivní ekosystém, ze kterého budou těžit všechny zúčastněné strany. [9]

Tokenizace však pro síť není nezbytně nutná. Mnoho projektů využívající privátní blockchain pro zdokonalení digitální infrastruktury v rámci průmyslových řešení tokeny vůbec nepoužívá. Tyto projekty, zejména pod konsorciem Hyperledger používají blockchain pouze k vytvoření struktury zápisu dat a jejich bezpečnému sdílení v rámci sítí.

5 Mechanismy autorizace bloků

Jedním z hlavních úkolů ve vývoji nových aplikací pro blockchain je hledání dokonalejších způsobů, jak bloky připojit k řetězci. Jedním ze základních parametrů kvality je rychlost autorizace bloků, versus úroveň zabezpečení. Jedná se o zásadní parametry při rozhodování, jaký typ algoritmu použít. Princip přidání bloku se v každém mechanizmu autorizace řeší jiným způsobem. Hlavním účelem algoritmu konsensu je dojít ke vnitřní dohodě mezi uživateli sítě. Uživatelé tak vytvářejí jednotnou historii transakcí, na které se dohodla majoritní většina sítě.

5.1 Problém Byzantských Generálů (BFT)

Problém Byzantských generálů je matematický problém, který byl publikován v roce 1982 kolektivem vědců Leslie Lamportem, Robertem Shostakem, and Marshalem Peasem. Tento problém se zabývá odhalováním chybných informací, které byly vytvořeny nesprávnou funkcí jednotlivých součástí systému. BFT se používá jako hodnota spolehlivosti sítě odolat a identifikovat katastrofické chyby v síti.

Samotný problém je nastíněný tak, že několik armád najednou obléhá město. Síly obou stran jsou téměř vyrovnané, ale pokud se obléhajícím armádám podaří synchronizovat jejich útok tak obránce města přemohou. Generálové se rozhodli, že si ráno pošlou zprávu, zda zaútočit, nebo se stáhnout. Proto generálové řeší, jak bezpečně a najednou doručit zprávu všem armádám. Existuje totiž možnost, že některý z generálů, nebo poslů se snaží útok zkompromitovat.

Tento problém vyřešil (i) tvůrce (i) Bitcoinu tak, že každý z generálů pošle všem zbývajícím generálům zprávu s rozhodnutím jak dále postupovat. Tak každý generál dostane stejný počet zpráv obsahující rozkaz k útoku, respektive stáhnutí. Převládající počet rozhodnutí určí jaké budou další kroky generálů.

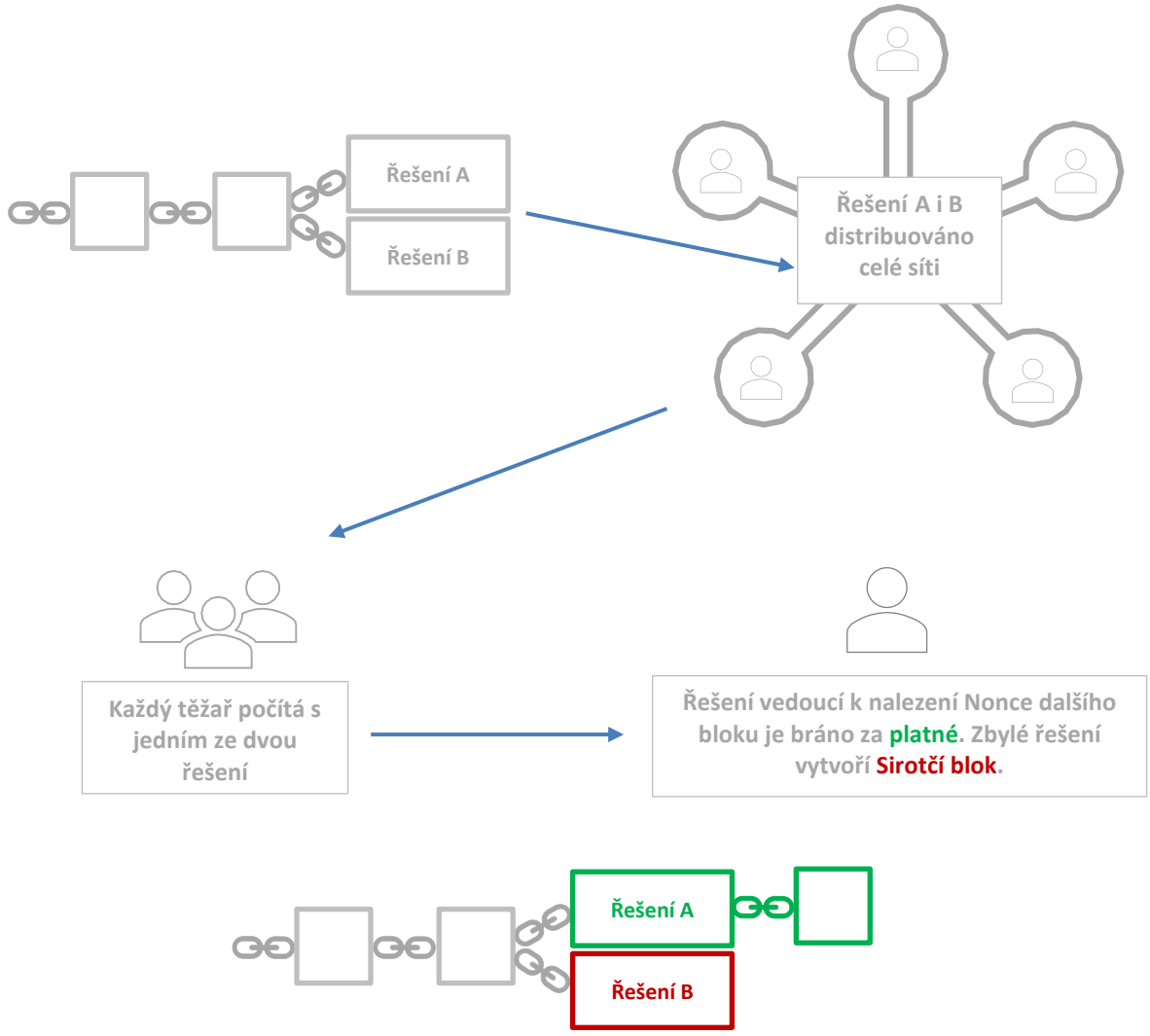
Řešení počítá s tím, že více jak polovina generálů, nebo poslíčků je důvěryhodná, což je známé v blockchainové technologii jako 51% útok.

Tento princip je využíván v blockchainu při přiřazování bloků. Pokud se někdo rozhodne škodit síti a vytvoří nový pozměněný blok, který bude distribuovat ostatním, síť dokáže na základě svých informací škodlivý blok rozpoznat a odmítnout.[11]

5.2 Proof of Work – PoW

Základní hybným prvkem těchto sítí jsou těžaři. Jsou to entity, které svojí prací dosahují konsensu a tím síti zabezpečují její správnou funkci. Těžaři sbírají všechny transakce a ukládají je do paměti, tzv. mempoolu (memory pool). Mezitím, co sbírají informace o transakcích, tyto transakce kontrolují a přidávají je do mempoolu, který představuje zárodek nového bloku. Jakmile je mempool plný, začne těžař zjišťovat jaká je Nonce pro vytvoření bloku. Když je Nonce nalezena, blok je vyřešen a opatřen Hashem. Následně je přidán do lokálního řetězce těžaře a rozdistribuován všem uživatelům. Blok ostatní uživatelé schválí přidáním bloku do svých privátních kopií řetězců. Jakmile je přidán více než 50% sítě, je blok považován za pravdivý. Následně je tvůrce bloku za svoji práci odměněn kryptoměnou. Přidání bloku do řetězce trvá u každého blockchainu jinak, například u Bitcoinu je to až 10 minut, což výrazně snižuje jeho využitelnost. Šance, že těžař vytěží další blok je přímo úměrný procesní síle, kterou těžař vynaloží. V praxi by to mělo znamenat, že pokud těžař vlastní desetinu procesní síly sítě, je schopen vytěžit každý desátý blok. Zároveň však jedna entita nesmí vlastnit více než 50% výpočetní síly celé sítě. V takovém případě by získal monopol na přidávání bloků a mohl by začít potvrzovat nepravdivé transakce. Všechny informace v mempoolu jsou po přiřazení bloku smazány a začíná se plnit novými transakcemi patřící do dalšího bloku. Tímto se v síti dosáhne konsensu ve všech transakcích, které proběhly v celé historii blockchainu. Pokud se stane, že jeden blok je nalezen dvěma těžaři ve stejnou chvíli, jsou oba bloky distribuovány celé síti. Těžaři začnou počítat další blok. Tím, že obě dvě verze bloku mají pravděpodobně rozdílné řešení, tzn. jejich Hash se liší, tak i následné bloky se musí lišit. Který následující blok je následně vyřešen jako první, je přidán do řetězce, aby vznikla jednotná verze a blok bez navázaní není brán v potaz, říká se mu „Orphan block“ (sirotčí blok). [12]

Protokol Proof of Work je nejbezpečnější a nejvíce demokratický typ konsensu sítě, avšak spotřebovává značné množství energie. Přidávání bloků do řetězce je moc pomalé, proto bude tento způsob přidávání bloků nahrazen, nebo výrazně modifikován.



Obrázek 6 Řešení problému sirotčího bloku [12]

5.3 Proof of Stake – PoS

V tomto algoritmu konsensu, se účastníci sítě podílejí na schvalování transakcí a jsou za přidávání bloků odměňováni, stejně jako u PoW (proof of Work). Způsob jakým jsou uživatelé vybírání k uzavření bloku je založen na pseudo-náhodném výběru mezi těmi kdo do sítě investují nejvíce peněz. Tím je zajištěno, že na funkci a bezpečí sítě mají největší zájem. Uživatel, který se chce účastnit vytváření bloku přesune své finance do části sítě s názvem Validator pool. Zde jsou finance zablokovány do té doby, než se blok uzavře. Částka investovaná do Validator poolu je přímo úměrná šanci, kterou má uživatel na připojení dalšího

bloku. Analogie v reálném světě je tombola. Čím poukazů soutěžící získá, tím větší má šanci na výhru hlavní ceny.

Pokud by však validátor chtěl škodit síti a začal verifikovat transakce, které nejsou podložené, hrozily by mu sankce v podobě odebrání aktiv ve Validator poolu. Kvůli tomu je nutné, aby u každého bloku bylo jasné, který validátor jej přidal. Na rozdíl od PoW nevyžaduje tolik výpočetní energie a má vysokou rychlost transakcí, ale na druhou stranu je jednodušší systém ovládnout. [12]

5.4 Delegated Proof of Stake – DPoS

Delegated Proof of Stake byl vymyšlen americkým softwarovým developerem Danielem Larimerem. Tento druh konsensu je často nazýván jako nejdemokratičtější způsob rozhodování o blockchainové síti. Stejně jako při Proof of Stake největší slovo v síti má ten kdo vlastní největší část aktiv, jinak můžeme říci, že má největší zájem o udržení důvěryhodné sítě. Tím je zaručeno, že jeho investice neztratí hodnotu. V síti jsou voleni Witnesses (svědci) a Delegates (delegáti). Podle typu sítě je využíváno 21-101 svědků, kteří následně získají právo uzavírat bloky. Volby svědků se může účastnit každý uživatel sítě. Na základě hodnoty vlastnictví v síti má jeho hlas přímo úměrnou váhu. Zvolení delegáti jsou následně automaticky vyzíváni k uzavření bloku. Svědek je za uzavřený blok odměněn jak finančně, tak získává důvěryhodnost, která mu při další volbě pomáhá k opětovnému zvolení. Jakmile se svědkovi nepodaří uzavřít blok, nebo se pokusí se sítí manipulovat, je sankciován finančně a zároveň je mu automaticky snížen koeficient důvěryhodnosti. Pro svědky je zásadní, aby po celou dobu jejich volebního období byli k síti připojeni. Jakmile se stane, že jsou od sítě odpojeni, jsou nahrazeni dalším svědkem v pořadí.

Delegáti na druhou stranu řídí systém v holistickém pohledu. Snaží se rozhodovat změnách v základním protokolu sítě, kontrolují výplaty svědkům, uzavřené bloky a intervaly, ve kterých jsou bloky přidávány. Jsou voleni stejným způsobem jako svědci, ale volby jsou mnohem méně časté. Delegáti nejsou za svoji práci placeni, to znamená, že musí být, bez jakéhokoliv nároku na odměnu, zainteresováni v rozvoji sítě. Díky efektivnímu způsobu výběru svědků není síť náročná na výpočetní sílu. Je rychlejší než Proof of Work a bezpečnější, než Proof of Stake. Na druhou stranu je stále náchylná na centralizaci. Pokud se více svědků rozhodne manipulovat s transakcemi, je možné síť ovládnout. [12]

5.5 Proof of Elapsed Time – PoET

Tento druh konsensu je založen na technologii firmy Intel Software Guard Extensions (SGX). Technologie byla představena v roce 2015. SGX funkce má zajistit Trusted Execution Enviroment(TEE), což můžeme volně přeložit jako důvěryhodné prostředí pro tvorbu kódu, nezávisle na typu využití sítě. SGX je hardwarový prvek, který vytváří sbírku instrukcí pro Central Processing Unit (CPU- Procesor), který je používán aplikací. Instrukce napomáhají CPU rozpoznat a izolovat důvěryhodné a nedůvěryhodné oblasti kódu a dat. V kostce vytváří podpis pravosti pro platformy a aplikace, které jsou napřímo napojeny na CPU a dohlíží, zda byly jejich procesy zahájeny a tvořeny v bezpečném prostředí. Tato funkce má podstatný vliv na funkcionalitu PoET, ale také tvoří vlastní bariéru pro vstup a limitaci jejich uživatelů. Umístění SGX je oddělené od uživatelů sítě, ale také od uživatelů s vyšší úrovní přístupu, kteří jsou administrátory této sítě. Aby nedošlo k její manipulaci. Jedná se o účinnější způsob PoW, kde je odstraněna nutnost vynaložení velké výpočetní síly pro získání jednoho bloku. Všichni uživatelé sítě musí vlastnit jednotku SGX. Každý zúčastněný získá náhodný časovač. Jakmile čas na jeho časovači uplyne, je tento uživatel autorizován k přidání bloku.

Při vstupu do sítě se musí uživatel prokázat jako věrohodný. To je splněno tak, že každý účastník si stáhne ze sítě iniciační kód, který následně ověří SGX a rozpošle účastníkům sítě. Jednotlivé uzly sítě (uživatelé) následně rozhodují zda tento kód přijmou, nebo odmítnou. Pokud je přijat, uživatel získá možnost se na síti podílet a v případě, že náhodný los času vyjde na něj dostane i možnost přidávat bloky.

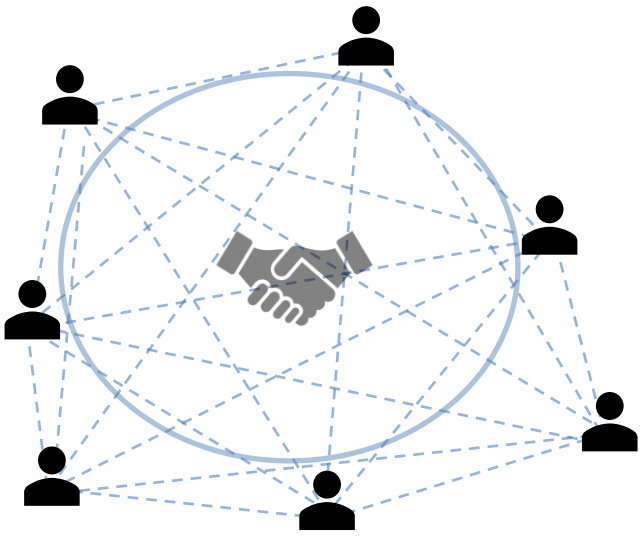
Druhou částí je samotný mechanismus konsensu. Po každém přidání bloku je účastníkům sítě rozeslán nový autorizovaný časovač. Díky tomu, že časy jsou rozděleny náhodně, zabráníme tomu, aby kdokoliv kdo chce síti uškodit přidával bloky častěji nežli ostatní. Výhody tohoto systému jsou rychlost a bezpečnost transakcí, jelikož všechny operace jsou kontrolovány technologií SGX. Je velmi efektivní pro využití v privátních blockchainech. Nevýhodou je však závislost na funkčnosti součástky třetí strany, tzn. firmy Intel, která tento validátor transakcí vyrábí. Privátní sítě nejsou kompletně decentralizované a závislost na produktu třetí firmy, není tak závažný problém. [13]

6 Základní rozdělení typů sítí

Původní myšlenka zabezpečených bloků s informacemi napojenými na sebe vznikla v roce 1991. Její tvůrci se snažili vytvořit systém s pevnou časovou známkou. Časová známka měla zabezpečit zpětné manipulaci se zápisy do sítě, tím pádem by byli jedinečné a nenahraditelné. V průběhu let se touto technologií začaly zabývat další průkopníci, buď samostatně, nebo v pracovních skupinách. Postupem času se vyvinulo základní rozdělení decentralizovaných sítí, které je možné zařadit do tří větví. Třemi typy blockchainových sítí jsou veřejný (skutečný decentralizovaný), privátní (jinak korporátní, nebo podnikový) a hybridní blockchain.

6.1 Veřejné sítě

Veřejné sítě jsou navrhnuté tak, aby se všechny subjekty mohly stejnou měrou podílet na dění v síti. Subjekty jsou myšleni uživatelé, těžaři, developeři i členové komunity. Všechny transakce jsou transparentní a všechny uzly sítě je kontrolují a potvrzují. Veřejné blockchainy jsou plně decentralizované. Nikdo, jako jedinec, či entita, nemůže kontrolovat, či ovlivňovat pořadí, v jakém jsou transakce do bloků zapisovány a jsou resistentní proti cenzuře. To je způsobené tím, že každý člen, bez ohledu na vzdělání, národnosti, nebo lokaci je na síti rovnocenným účastníkem. Je prakticky nemožné, aby byla veřejná síť zakázaná, ovládnutá, či kontrolována veřejnými orgány. Transakce prováděné v rámci veřejných sítí jsou viditelné všem účastníkům sítě, takže jsou aktivity uživatel zcela transparentní. Bezpečnost sítě je zajištěna silnými mechanismy autorizace, které jsou na druhou stranu pomalé a energeticky náročné. [14]



Obrázek 7 Veřejná síť [Autor]

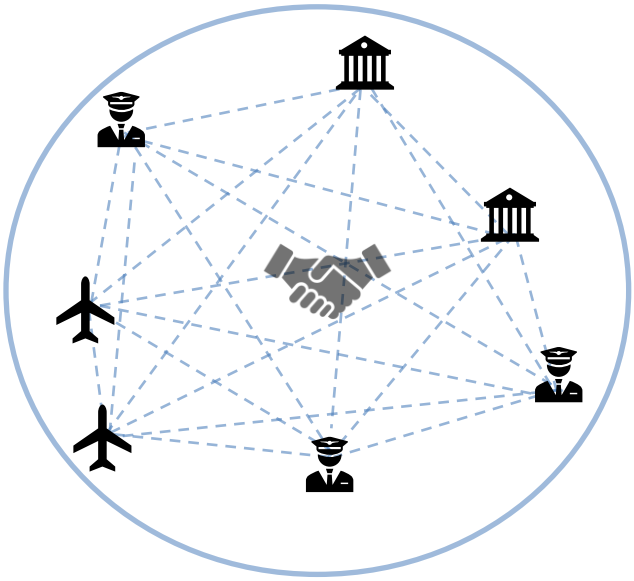
6.1.1 Ethereum

V roce 2013 vznikl blockchain nazvaný Ethereum. Jedná se o open – source platformu navrženou dvaceti dvou letým programátorem Vitalkem Buterinem. Ethereum změnilo smýšlení o blockchainových sítích. Hlavní změnou je implementace Smart kontraktů a s možnost zápisu jiných dat, než pouze účetních záznamů. Smart kontrakt běží v prostředí nazvaném Ethereum Virtual Machine a je zpřístupněný všem uživatelům. Jedná se zatím o jedinou veřejnou síť s možností využití v průmyslových odvětvích, potažmo v letectví. Přidávání bloků je prováděno pomocí PoW, ale do budoucna se počítá s adopcí mechanismu konsensu PoS, který by měl síť zrychlit a zároveň snížit energetické náklady na její provoz. Jejím tokenem je Ether, jako měna má podpořit tvorbu a provoz decentralizovaných aplikací. Připojení a provoz aplikací do sítě je zpoplatněné. Poplatky za každou transakci platí jak uživatel tak provozovatel. Výše poplatků je odvozena z velikosti dat, které jsou do blockchainu zapsány, proto je Ethereum nevýhodným nástrojem pro tvorbu komplexnějších průmyslových využití. Vývoj sítě je zaštítěn neprofitující organizací EEA (Ethereum Enterprise Alliance), která propojuje více jak 500 firem, univerzit, start-upů a expertů. Členy této aliance jsou i firmy Intel a Microsoft. Komunita poskytuje poradenství a nástroje pro tvorbu aplikací. Ethereum jako platforma je velice neohebná a pro reálné využití v letectví příliš anonymní. Ethereum však může sehrát roli jako ideální vzdělávací a testovací prostředí pro začínající projekty na tvorbu decentralizovaných aplikací pro letecký průmysl.[15]

6.2 Privátní sítě

Privátní blockchain je další přístup k tvorbě decentralizovaných sítí. Privátní blockchain má stejnou funkci jako veřejný Blockchain, je to bezpečné a rychlé sdílení dat v rámci sítě. Od veřejných sítí se liší hlavně omezeným přístupem uživatelů. Uživatelé musí pro vstup do privátních sítí splnit podmínky, které odráží její využití. Například při tvorbě privátního blockchainu pro civilní letectví, by účastníci sítě byly oficiální autority, letecké společnosti a letecký personál. Nutnost ověřování účastníků znamená, že účastníci sice ztrácejí naprostou anonymitu, ale zároveň je v rámci sítě získána větší důvěryhodnost. Zvýšená důvěryhodnost v rámci sítě umožňuje v privátních blockchainech zachovat soukromí aktivit a transakcí účastníků. Privátní sítě se tak nabízejí jako praktické řešení v řízení armády, správě institucí vymáhajících právo, ale také v zvyšování digitalizace civilního letectví. Zásadním parametrem pro využití korporátního blockchainu v průmyslových odvětvích, je rychlost uzavírání bloků. Korporátní blockchain v závislosti na důvěryhodnosti účastníků sítě nemá za potřebí využívat

robustní a energeticky náročné mechanismy k autorizaci bloků. Autorizace bloků je tak oproti veřejným blockchainům mnohem efektivnější a ekonomičtější. [14]



Obrázek 8 Privátní síť [Autor]

6.2.1 Hyperledger Fabric

Nadace Linux se zaměřila na tvorbu open-source konsorcia, které se zaměřuje na využití Blockchainových technologiích napříč průmyslovými odvětvími, který se nazývá Hyperledger. Hyperledger Fabric je jedním z řešení privátních sítí. Hyperledger Fabric díky svému softwaru pomáhá developerům a firmám stavět jejich byznys okolo platformy a rámců, které jim nabízí. Jedná se o nadnárodní kolaboraci firem podílejících se na stavbě systémů využívajících blockchain. Nabízí mnohá řešení na stavbu vysoko-škálovatelných, decentralizovaných aplikací. Hyperledger má za cíl působit jako osvěta veřejnosti v technologii blockchainu. Jedná se o jakýsi inkubátor ve stavbě průmyslových řešení využívajících blockchain. Konsorcium dalo vzniknout databázím generátorů Smart kontraktů, knihovnám, aplikacím a decentralizovaným rámcům, které mohou firmy pro vývoj sítí zdarma využívat. Fabric, jako mnohé další platformy blockchain nabízí využití Smart kontraktů a pomáhá členům v převádění zdrojů k zlepšení jejich efektivity. Je nutné, aby každý člen byl registrovaný jako uživatel, což zabraňuje anonymitě účastníků sítě. Tato technologie má ideální využití v zásobovacích řetězcích, uchovávání informací v leteckých společnostech, nebo ve finanční správě společností. Hyperledger Fabric dovoluje developerům zvolit pro svoji privátní síť jakýkoliv vyhovující typ konsensu. Síť je programovatelná v jazycích Go, JavaScript nebo Java. Pro své Smart kontrakty používá Chaincoin Algoritmus [16]

6.2.2 Hyperledger Sawtooth

Síť Hyperledger Sawtooth vznikla původně z iniciativy firmy Intel, nyní se komunita oddělila od své zakládající firmy a působí samostatně. Jedná se o vysoce flexibilní a modulární podnikový blockchain. Napomáhá firmám vytvořit, zprovoznit a udržovat digitální databáze. Tento Hyperledger si může firma vytvořit jako volný, nebo s nutností povolení pro jeho uživatele. Jeho architektura povoluje Smart kontrakty a zároveň se stará o to, aby byla tato platforma pro firmy dostatečně zabezpečená. Platforma dovoluje Blockchain naprogramovat jako decentralizovaný systém a má možnost vytvořit systém v různých programovacích jazycích. Blockchain pracuje na bázi potvrzování bloků pomocí dynamického konsensu, nejčastěji Proof of Elapsed Time (PoET), který je podrobněji vysvětlen v kapitole Mechanizmy autorizace bloků. PoET je algoritmus konsensu, který snižuje spotřebu energie a zdrojů. Procesy jsou díky němu efektivnější. Využívá se Sawtooth Validátoru a procesoru transakcí, který zvládá procesy, transakce a dále je distribuuje do peer-to-peer uzlů. Je využitelný v oblasti sledování produktů a digitálního vlastnictví. Sledování produktů by mohlo být využitelné pro výrobu a údržbu letadel. Dá se také využít v dodavatelských sítích velkých firem jako jsou Boeing a Airbus, kde jsou firmám dodávány velké kvantity součástek z různých zdrojů. Sawtooth podporuje více jazyků jako jsou Rust, Python, GO, nebo JavaSScript. Je možné naprogramovat na různé druhy konsensů, což dovoluje provozovateli, měnit pravidla sítě dle potřeb. Tento Dynamický konsensus povoluje využít typ PoET. [16]

6.2.3 Hyperledger Iroha

Spadá pod Linux Foundation. Jedná se o Blockchainovou platformu navrhnutou pro tvorbu důvěryhodných blockchainových sítí a decentralizovaných aplikací. Jedná se o platformu, která podporuje operační systémy Microsoft, macOS, i Linux. Tím se z ní stává ideální nástroj pro tvorbu IoT sítí. Stejně tak jako Hyperledger Sawtooth může být Iroha využit na správu dodavatelských řetězců a tvorby databáze pro údržbu letounů. Cílem tvůrců Hyperledgeru Iroha je vytvořit transparentnější privátní blockchain, při zachování bezpečnosti a rychlosti privátních sítí. Smart kontrakty jsou i zde velice významným nástrojem a fungují na stejných principech jako u Ethernea. [16]

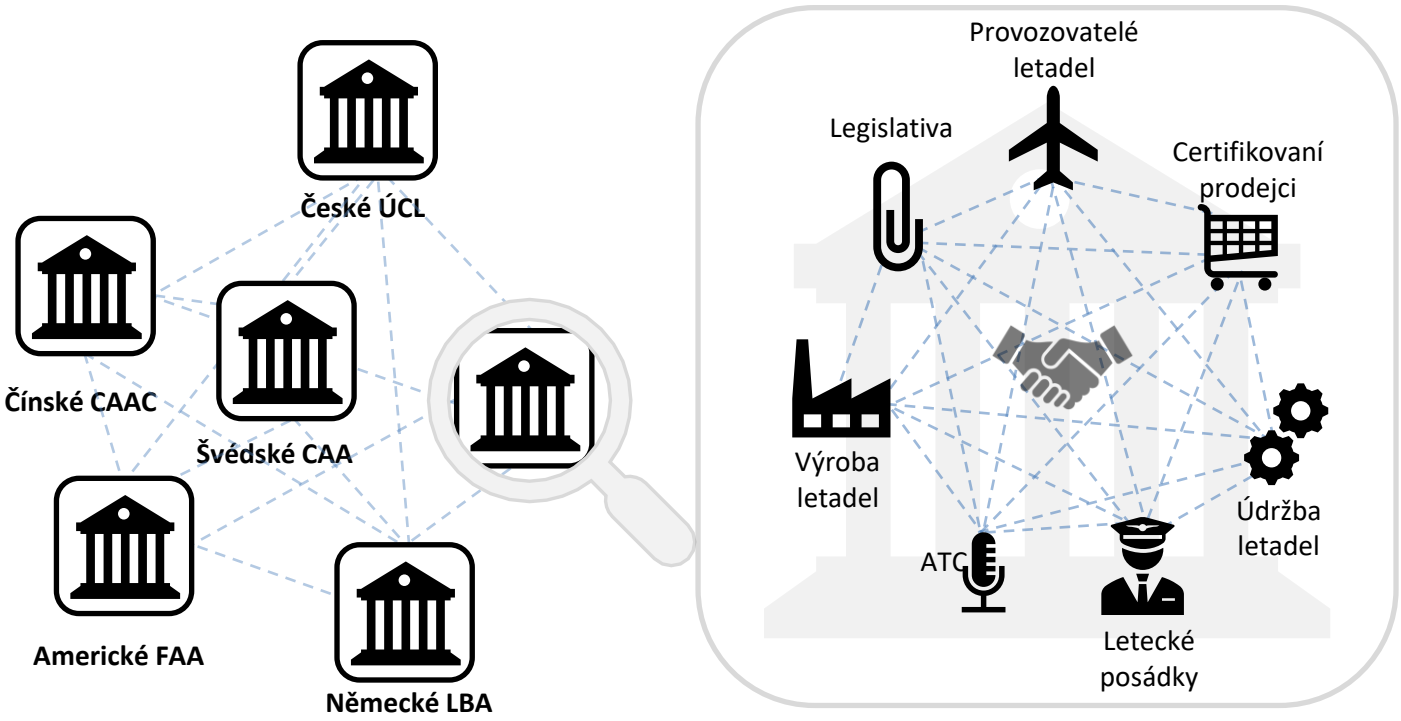
6.2.4 Quorum

Quorum byl navržen J.P. Morganem jako open-source architektura, kombinovaná s vlastnostmi Ethernea a dalšími implementacemi, které umožňují jeho lepší využití jako podnikového blockchainu. Nevysílá informace o transakcích všem uživatelům, ale pouze přímým

účastníkům transakcí. Dokáže zpracovat stovky transakcí za sekundu a povoluje využití Smart kontraktů. Quorum využívá konsensus založený na algoritmu vícenásobné volby, který má v sobě zabudovaný Smart kontrakt určující kdo, se může na volbě podílet. [16]

6.3 Hybridní sítě

Hybridní způsob stavby sítí je řešení, které má pro letectví největší potenciál. Kombinuje výhody veřejného a privátního blockchainu. Přináší bezpečí a transparentnost veřejného, v kombinaci s rychlostí a zabezpečením privátního blockchainu. Je složen ze dvou vrstev. Základní vrstva je veřejná. Její hlavní funkcí je působit jako decentralizovaná veřejná síť, spojující pod sebou uživatele a podniky. Podporuje jejich oficiální komunikaci, výměnu dokumentů a financí. Uživatelé a podniky pak tvoří druhou vrstvu hybridních sítí. Je jim dovoleno vytvářet samostatné privátní a veřejné blockchainy napojené na první veřejnou vrstvu. Toto zaručuje transparentnost v komunikaci mezi účastníky veřejného blockchainu, ale dovoluje v druhé vrstvě vytvářet zcela nezávislé ekosystémy. Účastníci sítě nemohou být anonymní, což přidává další bezpečnostní prvek. K uzavírání bloků ve veřejné vrstvě může používat jakýkoliv mechanizmus konsensu, ale dostatečnou rychlost, zabezpečení a nízkou spotřebu energie poskytne DPOS, nebo PoET. Využití hybridních sítí v letectví má potenciál. Velká většina států je sloučena pod organizací ICAO, ale každý kontinent, region, nebo stát má lehce rozdílnou legislativu. Hybridní sítě by mohly přinést platformu, na které by mohly všechny tyto samostatné prvky obchodovat, komunikovat a vyměňovat si oficiální dokumentaci. Tato vrstva by byla naprosto transparentní. Na ní by správní celky mohly držet veřejné informace o letounech, pilotech, nebo provozovatelích letadel. Data v sítích druhé vrstvy by spadala pod kompetenci jednotlivých správních oblastí a měla by privátní charakter. [14]



Obrázek 9 Hybridní síť[Autor]

6.3.1 Polkadot a Substrate

Patity Foundation spustila platformu pro tvorbu hybridní blockchainové sítě. Hlavní stavební jednotkou je veřejný blockchain Polkadot, který pod sebou sdružuje síť privátních a veřejných sítí. Oficiálním tokenem Polkadotu je DOT, který zabezpečuje možnost transakcí. Platformou pro tvorbu sítě je takzvaný Substrate, která v sobě obsahuje nástroje a návody pro jednoduchou tvorbu privátních i veřejných blockchainových sítí. Sítě vytvořené v nástroji Substrate jsou následně propojeny veřejnou sítí Polkadot, která dodává transakcím známku důvěryhodnosti pomocí externího mechanismu konsensu. Polkadot podporuje propojení se sítí Ethereum, takže je možné využívat jak aplikace tak kryptoměnu pohánějící Ethereum. Substrate dovoluje developerům vytvářet sítě a průběžně aktualizovat autorizační mechanismy a nastavení sítě. Dále dovoluje developerům tvořit nejen standardní aplikace, ale i takzvané webové aplikace. Webové aplikace jsou pro developery velmi výhodný nástroj. Dovoluje tvůrcům vytvářet aplikace, které je možné naprogramovat pouze v jedné verzi. Ta bude fungovat na všech zařízeních připojených k síti. Tvůrci aplikací nemusí za používání blockchainu platit síti, což dovoluje developerům vytvářet aplikace zpracovávající více dat. Tato platforma nabízí skutečně výhodné řešení pro startující projekty, které by mohly vznikat na

univerzitách. Jedná se o jednoduchý nástroj, ve kterém se dají testovat možnosti propojení vícero sítí pod jednou střechou. [17]

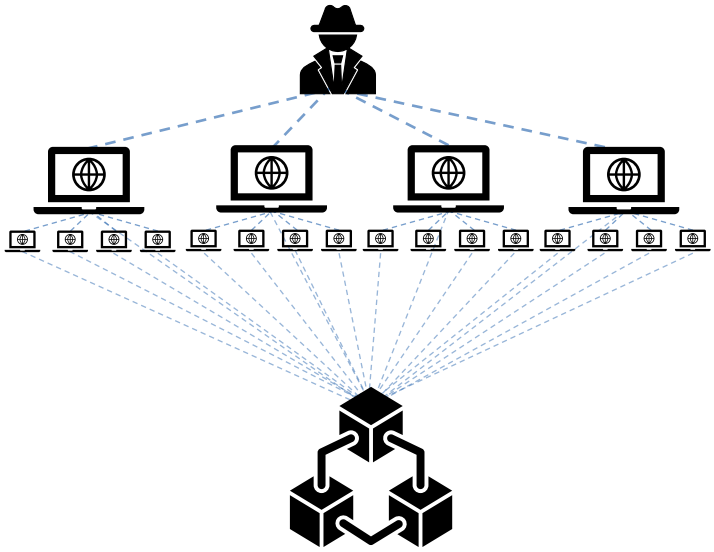
7 Nebezpečí útoků

V dnešní době se informace stávají, čím dál tím mocnější zbraní. Proto je důležité jakost informací efektivně ověřovat a chránit. Ne jinak je tomu i v blockchainových technologiích. U Blockchainových sítí v zásadě platí, že čím více uživatelů síť používá, tím menší je riziko manipulace s informacemi. Avšak existuje riziko útoku na síť, který způsobí její kritické selhání.

7.1 DDOS Útok

DOS Útok je ve výpočetních technologiích akronym pro Denial-of-Service. Hlavním cílem útoku je znemožnit uživatelům používat síť přetížením sítě. Útočník zaplaví síť obrovským počtem požadavků, které nebude možné zpracovávat a tím přestane plnit své základní funkce. V případě jednodušší formy útoku DOS (Denial-Of-Service), vyšle útočník požadavky pouze z jednoho uživatelského účtu. Tomuto útoku se dá poměrně jednoduše zabránit zablokováním IP adresy, která posílá nadměrný počet neopodstatněných požadavků. DDOS (Distributed Denial-of-Service) je mnohem sofistikovanější útok a tím pádem je i mnohem náročnější mu zabránit. V tomto případě se útočník naboural do více zařízení, ze kterých následně pomocí vícero IP adres zahlcuje síť. V takovém případě je mnohonásobně náročnější rozeznat pravdivost a nepravdivost požadavků, které jsou do sítě zasílány.[18]

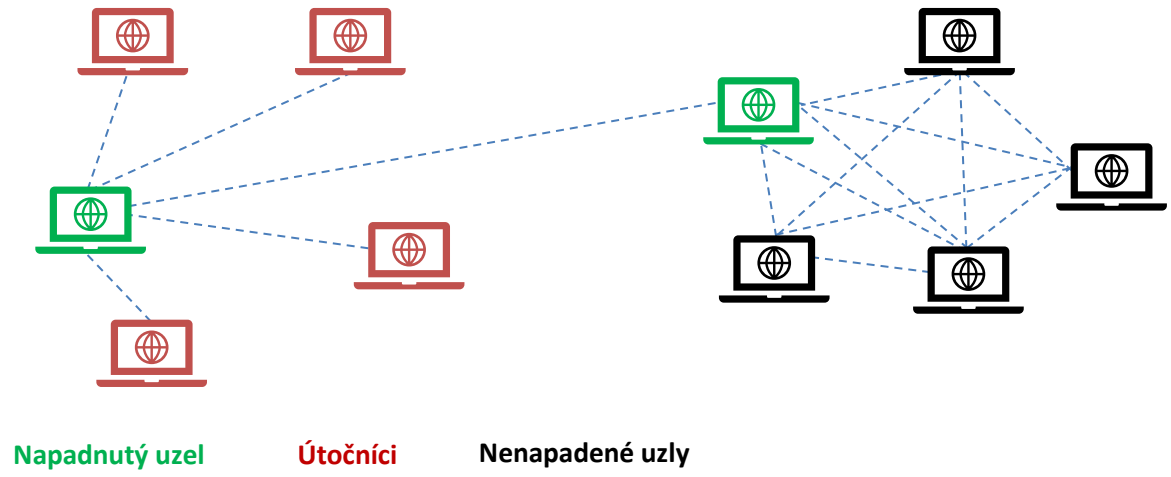
Tento útok je v blockchainové technologii navíc velice zrádný i ze samotné filozofie blockchainů, kde všechny požadavky uživatelů musí být považovány za právoplatný požadavek, který nesmí být nijak cenzurovaný a regulovaný. Na obranu sítě bychom museli vytvořit kritéria filtrování blockchainů a tím by vznikl nebezpečný precedens cenzury, při němž ztrácíme jednu z hlavních vlastností sítě. [18]



Obrázek 10 DDOS Útok [18]

7.2 Sybil útok

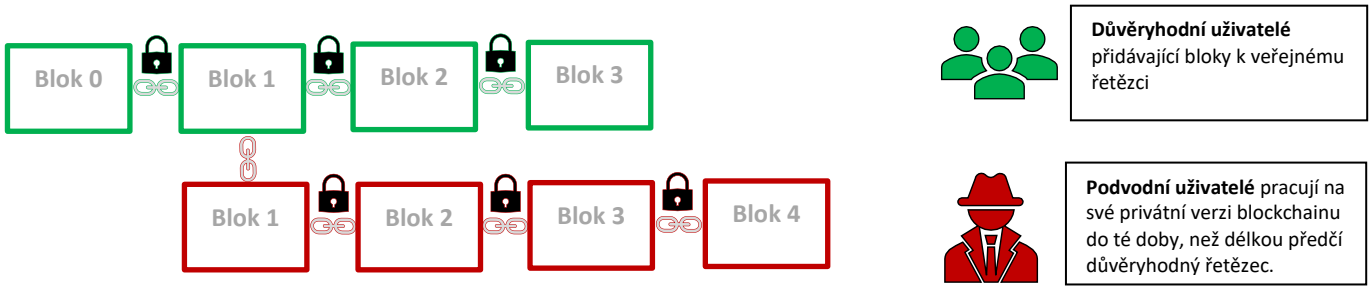
Sybil útok je pokus o manipulaci v jakýchkoliv peer-to-peer sítích. V síti je vytvořeno vícero nepravých uživatelských identit, které působí na venek jako normální uživatelé, ale společně pracují na manipulaci sítě. Tato varianta je zvláště nebezpečná, pokud se bavíme o blockchainech, které jsou založeny na hlasování. V dnešní době jsou tyto útoky nejvíce využívány na sociálních sítích, kdy se jedna entita, pomocí mnoha falešných účtů, ovládnout diskuze, či ovlivnit veřejné mínění v diskuzích. Jeden z druhů Sybil útoků je Eclipse útok, při kterém je uživateli sítě zamezeno přijímat a odesílat zprávy. Je však útočníky nastavena falešná komunikace. Útočník vytvoří falešné uživatelské účty, které přímo komunikují s napadeným uživatelem a ovlivňují jeho funkčnost v síti. Jedním ze způsobů jak zamezit tomuto útoku je nutnost platby za každý účet. Cena, však musí být velmi opatrně nastavená tak, aby se normálním uživatelům vyplatilo k síti připojit a falešným uživatelům nevyplatilo, byť i krátkodobě, do tvorby účtů zainvestovat. [18]



Obrázek 11 Vizualizace Sybil útoku [18]

7.3 51% útok

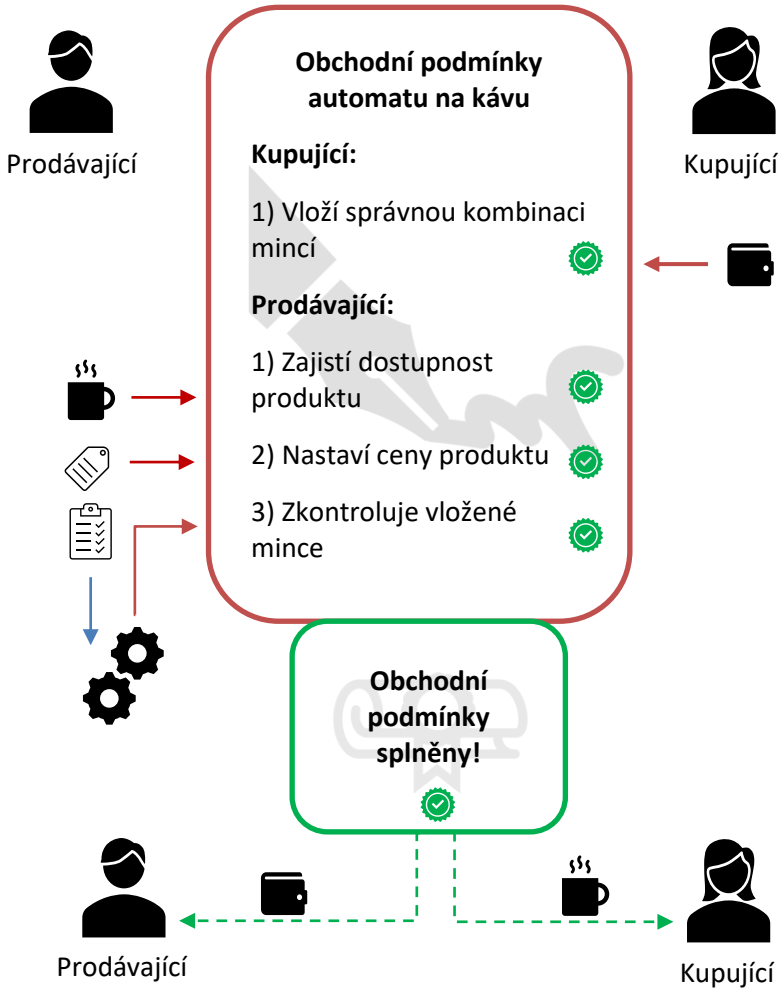
Útok 51% je nejznámějším útokem v blockchainových sítích. Cílem tohoto útoku je, hlavně v kryptoměnových blockchainech, zajistit útočníkovi možnost dvojí útraty. Popřípadě v sítích obsahujících citlivé informace vložit do systému falešná data. Útočník se pokusí v jednu chvíli uzavřít blok, ale zároveň začne pracovat na uzavírání dalších bloků na kopii svého řetězce. Nejprve nenahlásí změnu majitele kryptoměny a tím vytvoří dvojitý řetězec. Nově vzniklá část řetězce se nazývá privátní řetězec. Pokud tento uživatel, nebo skupina uživatelů, disponuje výpočetní sílou větší než 50% sítě, zmanipulovaný privátní řetězec bude růst rychleji než původní, pravdivý. Zlomový moment přichází ve chvíli, kdy nepravý řetězec je delší než původní. Blockchainové sítě totiž vždy akceptují jen jednu verzi řetězce a to vždy tu nejdelší. Ve chvíli kdy zmanipulovaný řetězec je delší než-li původní řetězec, je distribuován všem uživatelům. Uživatelé následně adoptují nepravou verzi a začnou k ní připojovat nové bloky. Tento útok naprosto znehodnotí celou databázi a již jí není možné nadále důvěřovat. Tomuto problému se dá předejít penalizací při přidávání více bloků naráz. Protože v síti není žádný legitimní důvod, aby bylo přidáváno více bloků najednou. Tím se odměna za manipulaci s řetězcem tak prodraží, že útočník snad nebude mít důvod tyto útoky provádět. [18]



Obrázek 12 51% Útok

8 Smart kontrakt

Blockchain je navržený tak, aby společně s daty mohl zahrnout do svého kódu také další programy. Jedním z takových programů je Smart kontrakt. Smart kontrakt je funkce nejčastěji používaná k automatické exekuci obchodní dohody. V reálném světě je nejjednodušší analogií Smart kontraktu automat na kávu. Obchodní styk je uskutečňován mezi kupujícím a subjektem provozujícím automat. Automat zastává funkci Smart kontraktu. Jsou v něm nastavené podmínky, které určují pravidla transakce. Podmínky pro kupujícího jsou vložit správný počet mincí do automatu. Jakmile je vložen správný obnos peněz má automat za úkol splnit své podmínky a těmi je vydat kupujícímu určený produkt. Díky automatu je proces prodeje kávy zbaven lidského prostředníka. Zbavením se prostředníka, je dosaženo zlevnění, zefektivnění a standardizaci procesu výdeje kávy. V průmyslových využitích se však Smart kontraktů dá využít nejen na vypořádání finančních transakcí, ale i na sběr a výměnu dat.



Obrázek 13 Analogie automatu na kávu, jako Smart kontraktu [Autor]

8.1 Oracle

Aby bylo možné vyhodnotit plnění podmínek Smart kontraktu, je potřeba zabudovat do sítě kontrolní článek. Funkci kontrolního článku plní ve Smart kontraktu jeden, ideálně více prvků, nazývajících se Oracle. Oracle sbírá informace z okolního světa a dodává je Smart kontraktům. Smart kontrakt díky nim vyhodnotí, zda podmínky uzavření smlouvy byly splněny, nebo nikoliv. Aby byl zdroj informací důvěryhodný nesmí být náchylný k manipulaci. V analogii automatu na kávu je Oraclem systém vyhodnocující hodnotu vložených mincí. Mince je zkoumána až sedmnácti parametry. Systém zkoumá materiál a rytí pomocí vysokofrekvenčního měření, hmotnost, velikost a další parametry. Na konci procesu automat minci nepřijme, nebo přijme a přiřadí jí hodnotu. Důvěryhodnost je zde podpořena použitím více nezávislých měření, která mají svoje tolerance chyb. Na podobných principech pracují i Oracle v elektronickém světě. Základní vlastností Oracle musí být nezávislost, proto pro zvýšení bezpečnosti je nutné mít velký počet důvěryhodných a mezi sebou nepropojených kontrolních zdrojů. [19]

8.1.1 Software Oracle

Software Oracle hledá informace v internetových sítích a databázích. Informace přijímá z veřejně dostupných zdrojů. Převládající názor zdrojů iniciuje exekuci Smart kontraktu. Nevýhodou těchto zdrojů je narůstající počet nepravdivých informací kolujících internetem. Nastává nutnost nastavit funkční mechanizmus vybírání informačních zdrojů. Jednou z vizí blockchainových developerů je tvorba decentralizovaného internetu, kde by za pomoci digitálních identit bylo možné dohledat zdroje informací a vytvořit hodnocení jejich důvěryhodnosti. Software Oracle by v letecké dopravě představovali například programy FlightRadar24, nebo servery vyhodnocující počasí. Jako zdroj informací by mohly pomoci potvrzovat lety, nebo vyhodnocovat v jakých podmínkách byly letouny provozovány.[20]

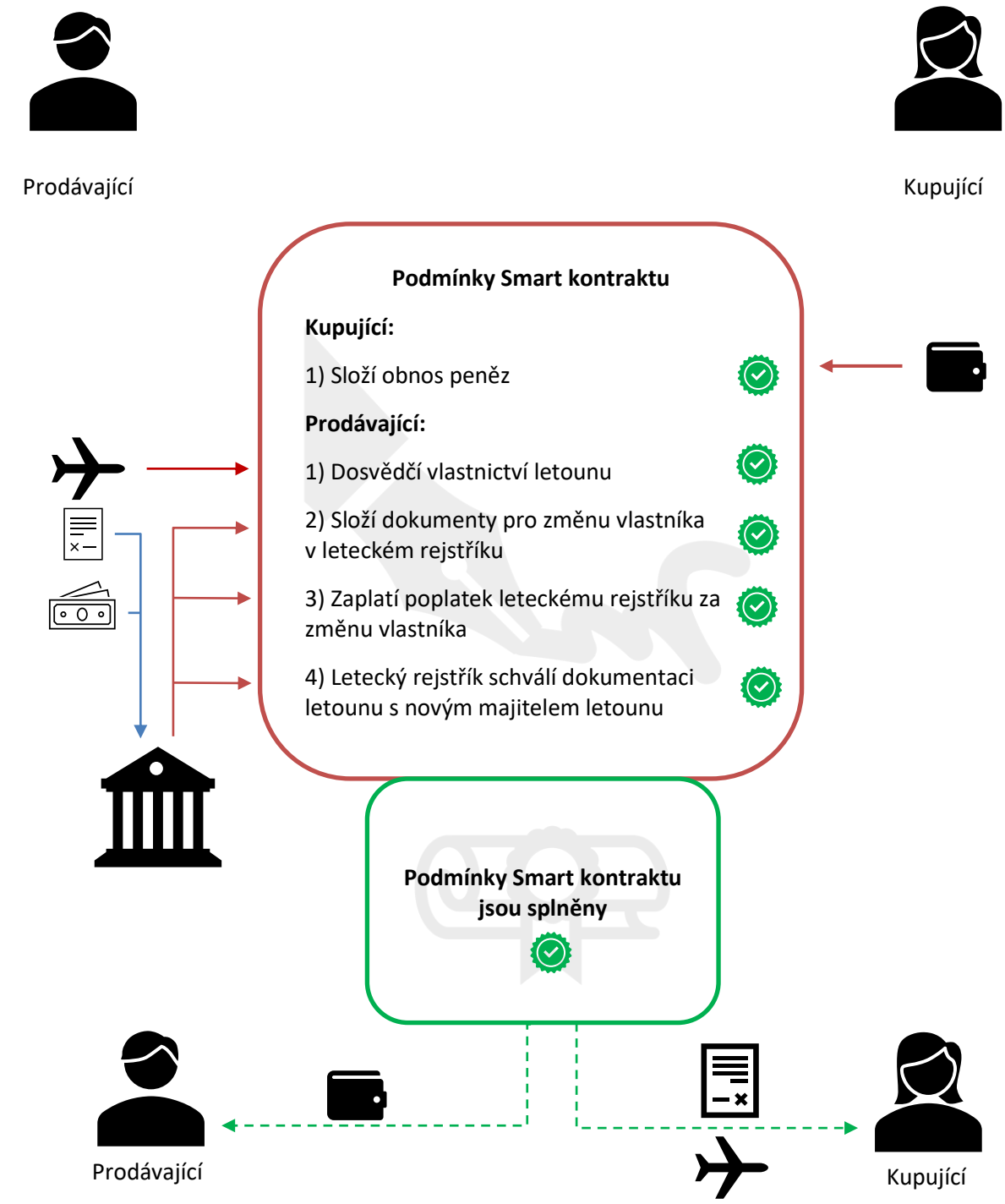
8.1.2 Hardware Oracle

Informace pro Smart kontrakt jsou odebírány sledováním vnějších a vnitřních vlivů pomocí čidel a senzorů připevněných na sledovaném objektu. Na podobném principu funguje Internet věcí IoT (Internet Of Things). Internet věcí je síť inteligentních zařízení. Zařízení, za pomoci čidel zaznamenávat dění kolem sebe. Získaná data ze sledování následně pomocí naprogramovaných algoritmů vyhodnocují a doporučují další kroky. Tyto sítě využívají umělou inteligenci a umělou intuici, které pomáhají přístrojům v učícím procesu. Přispívají tím k rozvinutí reakcí na vzniklé externí podněty. Ve Smart kontraktech se dá těchto čidel využít pro dokonalou automatizaci procesů. Stejně jako u softwarových Oracle je však nutné, aby byly

hodnoty měřeny více nezávislými zdroji. V leteckém světě by hardware Oracle byla zařízení sledující stav letounů. Jednalo by se o čidla zaznamenávající fyzikální vlastnosti, ve kterých se součástky nachází. Na jejich základě by pak Smart kontrakty mohly vyhodnocovat, zda je nutné přistoupit ke kontrole, výměně a objednání nového náhradního dílu.[20]

8.2 Smart kontrakt pro využití brokerských služeb

Pokud kupujete nemovitost, letoun nebo jinou drahou komoditu, je velice často využíváno brokerských služeb. Jedná se o právnické osoby, které mají důvěru obou stran uzavírajících obchod. Brokeři zaštiťují aby proces proběhl podle dohodnutých pravidel. Každá z obchodujících stran přepíše majetek brokerovi, který po splnění podmínek obchod vypořádá. Brokeři slouží jako jistota pro případy, kdyby jedna z obchodujících stran měla v úmyslu nedodržet stanovené obchodní podmínky. Tím, že se jedná o renomované právnické osoby, které disponují vysokou důvěryhodností, je cena těchto služeb poměrně vysoká. Smart kontrakt v takových případech nahradí brokerské služby. Zprostředkovatelé brokerských služeb mají vloženou důvěryhodnost zkušenostmi a dlouho budovaným renomé. Blockchain má důvěryhodnost zabudovanou ve svém algoritmu, není ji proto nutné budovat, ale je automaticky implementovaná v jeho matematické podstatě. Pokud je nutné uskutečnit obchod můžeme k tomu využít Smart kontrakt, stačí nastavit kombinaci podmínek, které budou nezávisle kontrolovatelné Oraclem a následně transakce automaticky vypořádaná. Taková služba nám usnadní obchodní jednání a zároveň účastníky ochrání v případě nepředvídatelných situací, jako například může být bankrot brokera.



Obrázek 14 Smart kontrakt jako brokerská služba [Autor]

8.3 Smart kontrakt pro dodavatelské řetězce

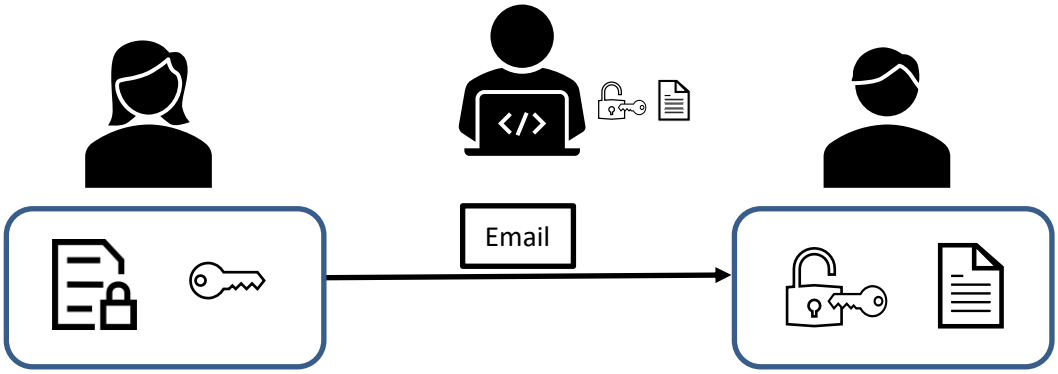
Dodavatelské řetězce se stávají čím dále složitější sítí, ve které sami koncový výrobci mají malou šanci dohledat původ součástek, ze kterých jsou finální produkty tvořeny. Každý složitější stroj je sestaven z tisíců a více součástek pocházejících z různých koutů planety. Stejně to zcela jistě platí o dopravních letounech. Dopravní letouny se skládají z milionů samostatných součástek, které pocházejí od stovek dodavatelů, kteří mají dále své subdodavatele. Tato komplexnost tvoří obrovský potenciál pro chybovost, která může mít fatální důsledky. Zabudováním procesů kontroly za pomoci Internetu věcí, je možné nastavit dokonale sledovatelnou historii všech komponentů letadla. Bude známa nejen jejich lokace, ale může být pomocí zabudovaných čidel sledováno i zacházení s nákladem, nebo jaké budou další kroky v dodání materiálu. Smart kontrakty mohou pomoci získat absolutní kontrolu do dodavatelských řetězců a velice zefektivnit jejich funkčnost.

8.4 Výzvy Smart kontraktu

Největší výzvou pro blockchainové sítě je, v současné době, přiřazení právní hodnoty kontraktům, které proběhly pouze ve virtuálním světě. Je nutné si uvědomit, že pro napsání smlouvy v reálném světě je zapotřebí člověka, který mnoho let studoval rámec práva potřebný pro pokrytí všech úskalí a šedých míst. Nyní si představme, že bude zapotřebí člověk, který se nejen vyzná v legislativě, ale bude nucen mít také vzdělání v oboru IT, aby byl schopen vytvořit smluvní program, který by nabyl skutečnou právní hodnotu. Další velkou překážkou je zajistit data, která jsou důvěryhodná, aby podle nich mohl Smart kontrakt vyhodnotit splnění, či nesplnění podmínek. V podstatě musíme naučit program, aby kontroloval věci v reálném světě. Bohužel i v tomto případě nastává problém. Co když někdo s nekalými úmysly napadne databázi úřadu civilního letectví. Proto jediný Oracle není dostatečný. Aby Oracle byl důvěryhodný zdroj informací je nutné, aby informace přicházeli z několika nezávislých zdrojů.

9 Aplikace Wallet

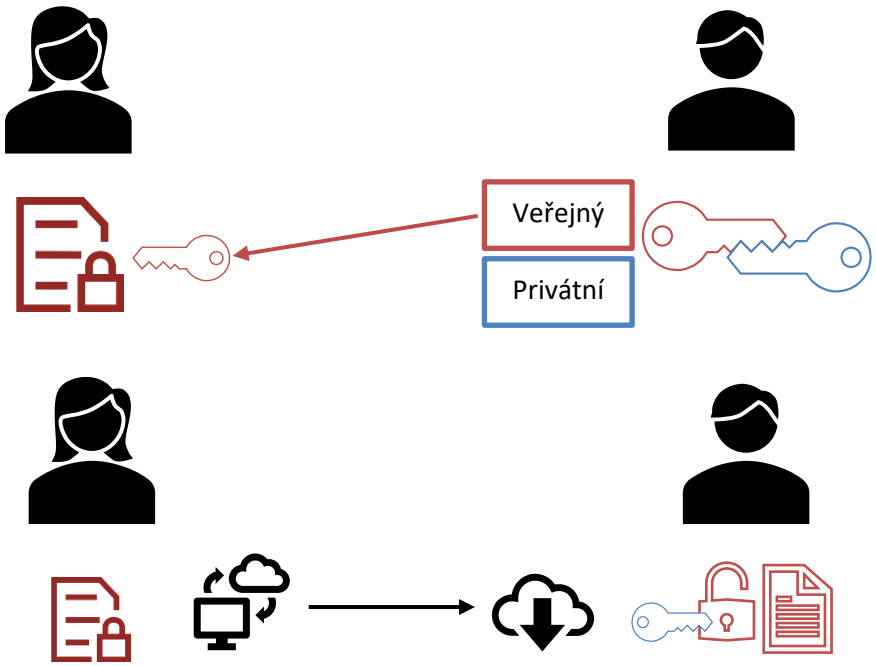
Zásadní pro aplikaci Wallet je pochopení principů symetrické a asymetrické kryptografie. Symetrická kryptografie povoluje zašifrovat dokument a zároveň k němu vytvořit klíč. Tento klíč je unikátní a dovoluje jeho držiteli dokument otevřít. Pokud tvůrce chce soubor s někým sdílet, musí poslat jak samotný dokument, tak klíč k jeho dešifrování. Při posílání klíče se však odesílatel vystavujeme vysokému riziku, že se dokument i klíč dostanou do rukou třetí osoby. Proto si musí odesílatel souboru být naprosto jistý, že komunikační kanál není diskriminovaný.



Obrázek 15 Symetrická kryptografie [Autor]

Asymetrická kryptografie používaná v blockchainových sítích nám může toto riziko výrazně snížit. Každý uživatel sítě má svůj unikátní privátní i veřejný klíč. Dvojice klíčů je k sobě pevně matematicky vázána. Veřejný klíč má dvě základní funkce. Funguje jako adresa a zároveň je hlavní součástí šifrovacího procesu. Privátní klíč pak dovoluje dešifrovat soubory, zakódované pomocí veřejného klíče, ke kterému patří.

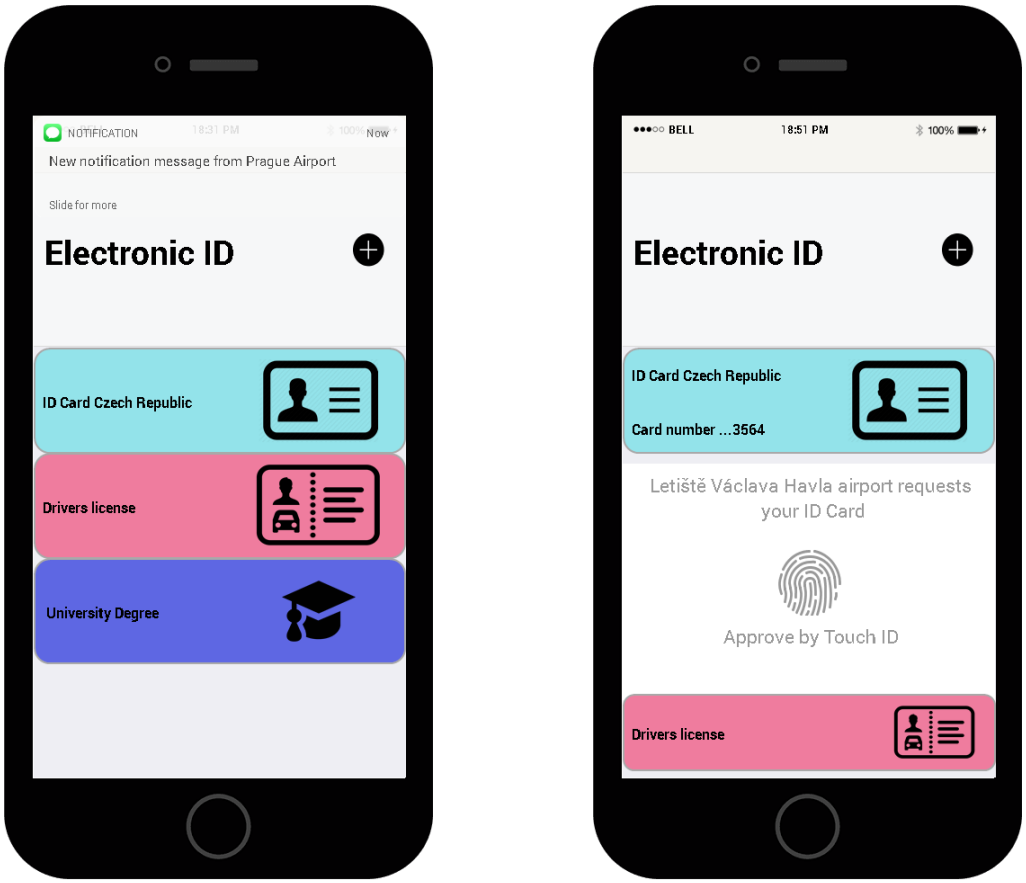
Pokud se odesílatel se rozhodne sdílet soubor cenných dat, zažádá adresáta o jeho veřejný klíč. Jakmile je mu poskytnut veřejný klíč je použit k zašifrování souboru. Takto zabezpečený soubor může odesílatel poslat přes jakýkoliv komunikační kanál, který zajistí doručení adresátovi. Příjemce následně pomocí svého privátního klíče má možnost soubor otevřít. Výhoda asymetrické kryptografie spočívá v tom, že k cenným datům se nedostane nikdo jiný než vlastník privátního klíče příjemce. Soubory tak mohou být veřejně dostupné, ale k jejich otevření bude mít právo pouze jeden uživatel. [21]



Obrázek 16 Asymetrická kryptografie [Autor]

Aby tato výměna dat mohla probíhat je nutné zajistit dvě základní podmínky. Oba uživatelé musí používat aplikaci Wallet, který danou transakci podporují a oba účastníci výměny dat musí být připojeni k síti. Aplikace by měla mít jednoduché uživatelské prostředí, kde uživatelé spravují své privátní a veřejné klíče. Pokud uživatel pracuje s kryptoměnami, skladuje informace o bilanci svého účtu. V implementaci pro elektronickou identitu se zde budou uchovávat osobní doklady, licence, nebo certifikáty. Aplikace může podporovat autorizaci pomocí biometrických údajů v podobě otisků prstů, nebo rozpoznávání tváře. V případě, žádosti o přístup k datům uživatele, by byla jednoduše vygenerována žádost přes veřejnou část klíče uživatele. Na uživatelově zařízení by se v případě, že je připojen k síti, vytvořila notifikace. Notifikace by obsahovala informace o žadateli a o rozsahu dat, ke kterým mu dáváme přístup. Uživatel by potvrzením mohl transakci přijmout, nebo naopak zamítnout. Na vizualizaci níže, na je na levo znázorněna domovská stránka aplikace. Jsou zde pro názornou ukázku přidány tři dokumenty dokazující naši identitu. Občanský průkaz, řidičský průkaz a univerzitní diplom. Dokumenty jsou digitální formou fyzických dokumentů. Stejně tak jako fyzické dokumenty, jsou elektronické dokumenty vydávány důvěryhodnou autoritou, například Ministerstvem vnitra ČR, nebo univerzitou. Zároveň v horní části obrazovky je možné vidět notifikaci. Notifikace uživatele informuje, že Letiště Praha žádá přístup k elektronickému Občanskému průkazu. Po zvolení elektronického občanského průkazu v aplikaci, má uživatel možnost přístup k dokladu poskytnout. Tedy

je pouze na uživateli, zda žadateli o informace důvěřuje, nebo nikoliv. Spolu s rozvojem elektronické identity bude nutné vyřešit i otázku hodnocení důvěryhodných ověřovatelů identity. Hodnocení by poskytlo uživateli informaci, zda je možné tomuto ověřovateli důvěřovat, nebo zda se poskytnutí osobních informací nedoporučuje. [21]



Obrázek 17 Vizualizace Aplikace Elektronického identity [Autor]

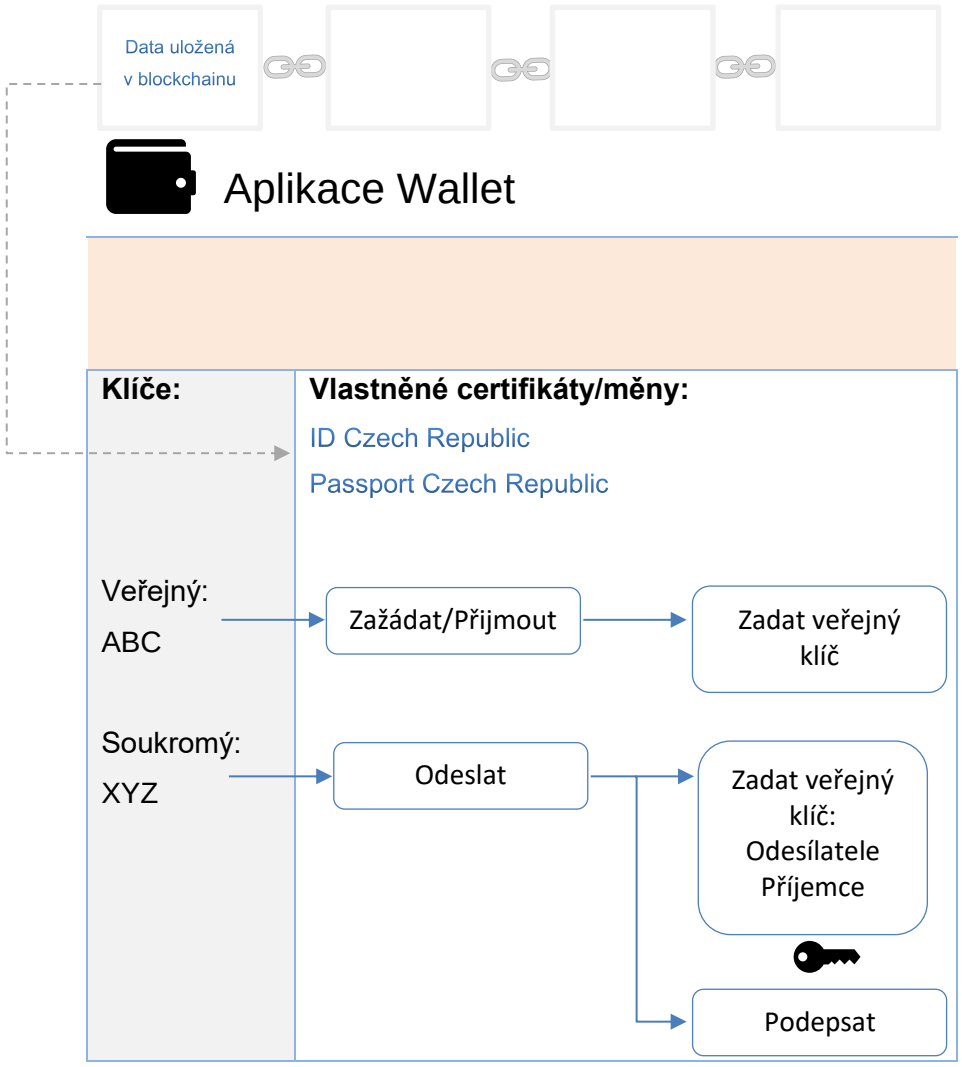
9.1 Struktura požadavků

Wallet je aplikace na generování, správu a skladování privátních a veřejných kryptografických klíčů, které dávají přístup informacím uloženým v blockchainu. V aplikaci však jsou uloženy pouze klíče. Data samotná jsou uložena v blocích na síti a distribuovaná všem uživatelům. Uživatelské rozhraní musí obsahovat tři základní funkce. Odeslat žádost, přijmout žádost, nebo zaslat finance, respektive data pomocí veřejného klíče.

Funkce odeslání žádosti pomůže uživateli vygenerovat požadavek s využitím veřejného klíče příjemce. Tento požadavek se následně zobrazí adresátovi v aplikaci Wallet. Adresát bude moci zkontrolovat, kdo požadavek poslal a co je jeho obsahem. V použití kryptoměn bude obsahem žádost o zablokování domluvené částky. Ve využití osobních dokumentů se může

jednat o informace ohledně jeho identity. Například zda je vysokoškolsky vzdělaný a jaká je jeho Alma mater. Ve veřejných sítích bude moci požadavky posílat každý uživatel, ve více škálovaných sítích pro oficiální komunikaci, budou moci požadavek posílat pouze organizace s dostatečným oprávněním. V příkladě elektronické identity, by požadavky mohly posílat pouze státní orgány a organizace je zastupující. V případě implementace pro elektronické cestovní doklady, by kontrola na letišti mohla zaslat na základě uživatelova veřejného klíče požadavek na identifikaci pomocí elektronického pasu, notifikace by ho následně zavedla do rozhraní aplikace Wallet.

Další funkcí, kterou uživatelské rozhraní musí obsahovat je možnost poskytnout data/finance bez předešlého požadavku. Stejně jako na bankovním účtu bude moci uživatel zaslat data/finance pomocí veřejného klíče. Pro příklad uživatel chce žádat o práci. Žadatel na stránkách pracovního úřadu najde nabídku práce. Součástí nabídky práce bude veřejný klíč zaměstnavatele a jaká data musí poskytnou, aby žádost byla zpracovaná. Uživatel otevře funkci poskytnou data. Zadá veřejný klíč a rozsah osobních údajů, které chce s příjemcem sdílet. Informace se automaticky vyplní. Vyplněná data poté podepíše pomocí hesla, nebo biometrických údajů a odešle je zaměstnavateli. Zaměstnavatel po přijetí bude moci automaticky odeslat čas a podmínky dalšího kola výběrového řízení. Výhoda této výměny dat je zabezpečené prostředí. Na rozdíl od elektronické pošty, nemůže nikdo jiný než adresát otevřít soubor s osobními údaji. Do jisté míry se zaměstnavatelé mohou krýt před zákonem o osobní ochraně a bude možné zaslat naprosto anonymní soubor informací obsahující pouze zda žadatel absolvoval vysokou školu, nebo jestli je vlastníkem řidičského průkazu typu B. [21]



Obrázek 18 Vizualizace procesů aplikace Wallet [Autor]

9.2 Manipulace s klíči

Jedním ze základních problémů fyzické formy dokumentů je možnost jejich ztráty a následné odcizení identity, nebo jiné zneužití osobních dat. Stejný problém však může nastat i s elektronickou verzí dokumentů a peněz. V zásadě existuje pět způsobů uschování privátního klíče. Každý z pěti způsobů má své silné a slabé stránky a záleží pouze na uživateli, který ze způsobů mu nejvíce vyhovuje. Bohužel uschování privátního klíče je stále nejslabší stránkou této technologie, pokud se třetí osobě podaří získat privátní klíč uživatele, má přístup ke všem informacím uloženým v síti. S rostoucí popularitou využívání biometrických údajů pro autorizovaný přístup je však možné, že se tento problém podaří vyřešit. Nevyhnutelně se tak

z našeho těla se stane unikátní privátní klíč. Privátní klíč, který se nebude nutné zálohovat a dramaticky se sníží možnost jeho odcizení, či ztráty.

9.3 Webové aplikace Wallet s nutností hostování

U hostovaných webových aplikacích Wallet je vkládána důvěra třetí straně, která kryptografické klíče uloží na svých serverech. Nejdříve je nutné si u těchto zprostředkovatelů služby vytvořit účet. Dalším krokem je zadání našeho privátního a veřejného klíče. Peněženky potom spárují tyto informace účtem. Následně je možné v rámci jejich rozhraní provádět transakce na blockchainech, se kterými zprostředkovatel služeb spolupracuje. Velkou výhodou je, že pokud neztratíme přístup na stránky webového zprostředkovatele služeb, nemůžeme klíče ztratit. V případě zapomenutí přihlašovacích údajů může uživatel pomocí jednoduché autorizace získat kontrolu nad svým účtem zpět. [22]

Nevýhodou je, že uživatel vkládá klíče do rukou třetí osoby. Což je citlivé primárně ze dvou důvodů. Nedostatečné kontroly nad manipulací s klíči a zároveň se zprostředkovatel služeb může stát cílem hackerského útoku. Databáze těchto serverů jsou velice lákavým cílem hackerů, kteří následně mohou získat kontrolu nad mnoha účty najednou. Dalším nebezpečím je možnost krachu serveru, nebo samotné firmy. Pokud klíče nezálohujeme jiným způsobem, tak jsou data uložená v blockchainu ztracená nadobro. [22]

9.4 Webové aplikace Wallet bez nutnosti hostování

Pro přístup do nich je nutné vložit privátní klíč při každém přihlášení. Jedná se o aplikace fungující jako plug- in do existujících webových prohlížečů. Vytvoří se klíčenka chráněná před podvodnými servery a umožňuje jednoduchý přístup do webových aplikací pomocí automatického vyplnění privátního klíče. Uživatel ukládá privátní klíč do počítače pomocí plug-in aplikace, která mu dávají jistou úroveň ochrany. Výhodou je jednoduchost použití, ale na druhou stranu pokud je počítač napaden, je veliká pravděpodobnost, že bude klíč zkopírován a odcizen. Proto je dobré soubor plug- inu, ze kterého se klíč načítá uložit na externí hard disk a připojovat ho k počítači pouze pokud ho plánujeme použít. Pokud je však zařízení ztraceno, je ztracen i přístup k našemu klíči. [22]

9.5 Mobilní aplikace Wallet

Mobilní aplikace Wallet nabízí uživateli možnost uložit svůj privátní klíč do telefonu. Přístup k němu získáme po zadání hesla, nebo po použití biometrických údajů pomocí Face ID, nebo

TouchID. Výhodou je uživatelsky přátelské prostředí s vysokou mírou zabezpečení, kterému ale stále hrozí nebezpečí hackerského útoku. Proto je nutné dodržovat uživatelskou hygienu a nedat útočníkům možnost se do zařízení dostat. Pokud zařízení ztratíme náš privátní klíč je ztracen a s tím i naše data. Existuje možnost nahrát klíč do internetové úschovny dat, jako je například iCloud, ale tím nahráváme citlivá data na servery, které jsou pod neustálým náporem hackerských útoků[22]

9.5.1 Fyzický privátní klíč

Idea fyzického privátního klíče spočívá ve vytisknutí jeho skutečného znění v papírové podobě. Všechny aplikace Wallet tuto možnost podporují. Fyzická kopie je ideální pro zálohování klíče v případě, že je ztracen přístup k aplikaci Wallet. Velice častý postup je uschování tohoto klíče do trezoru. Kde slouží jako záloha v případě, že je ztracen přístup k jeho digitální podobě. Následně je možné kód znova do aplikace vložit a pokračovat v jejím používání. [22]

9.6 Hardware aplikace Wallet

Hardware aplikace Wallet jsou specifické externí hard disky, které v sobě mají uloženou jak aplikaci tak privátní klíč. Aplikace je spustitelná pouze pokud vložíme hard disk do zařízení. Výhodou je, že aplikace i hard disk jsou zapojené do sítě pouze ve chvíle, kdy je využíváme. Zmenšuje se tím prostor pro hackerský útok. [22]

Typ	Lokace uložených informací	Kde je spuštěná aplikace	Příklady
Webová aplikace Wallet Nutnost hostování	Kryptografické klíče jsou uloženy třetí stranou	Na serveru třetí strany	Většina směnáren Coinbase, Binance, Bittrex atd.
Webová aplikace Wallet Bez nutnosti hostování	Uživatel má sám uložené kryptografické klíče	Ve webovém prohlížeči	MyEtherWallet
Mobilní aplikace Wallet	Klíče jsou uloženy na zařízení, na kterém máme nainstalovanou aplikaci	V zařízení na kterém je aplikace nainstalována	Swing, Arizen, Coinomi, Paytomat
Fyzický privátní klíč	Klíče jsou vytisknuté na papíře	Mohou být využity do všech typů peněženek	Generátor papírových privátních klíčů je možný pro většinu aplikací Wallet
Hardware aplikace Wallet	Klíče jsou uloženy na disku speciálního zařízení	Ve webovém prostředí, nebo v samostatném programu	Ledger, CoolWallet, xeeda, Trezor atd.

Obrázek 19 Výhody a nevýhody jednotlivých řešení uchovávání klíčů [22]

10 Správa digitální identity v letectví

V době, kdy se valná většina všech procesů okolo nás odehrává automaticky a online v reálném čase, je vhodné začít přemýšlet o možnosti vytvoření digitální identity, která by každého člověka provázela od narození. Naše identita je v současnosti specifikována rodným listem, občanským průkazem, pasem, složkou u doktora, řidičským průkazem, nebo diplomem z univerzity. Pokud se těmito dokumenty chceme identifikovat, musíme je mít ve fyzické podobě. V případě, že chceme prokazovat identitu v digitálním světě, je nutné osobní dokumenty naskenovat, nebo vyfotit a zaslat elektronickým komunikačními kanály. Elektronické komunikační kanály jsou však neustále exponovány útokům z vnějšího světa. Nejedná se však pouze o nebezpečí útoků, dalším problémem při poskytování digitalizované identity, je nastavení oboustranné důvěry mezi kontrolním článkem a uživatelem prokazujícím identitu. Kontrolní článek si musí být jistý, že odesílatel poskytuje pravou identitu. Zároveň odesílateli dokladu musí být zaručeno, že adresát data nezneužije a zároveň ji ochrání před útoky hackerů. Po odeslání uživatel ztrácí kontrolu nad dalším využitím a způsobem uchovávání svých citlivých dat. Takovýto postup skýtá mnoho třecích ploch, kde by mohlo dojít k odcizení identity. Zvyšující se četnost odcizení identity dala vzniknout zákonu GDPR, který řeší problematiku ochrany osobních údajů. Zákon vznikl na základě chybějící legislativy zabývající se prací s osobními daty. Řeší reálné problémy, které se vyskytly s nástupem moderních technologií, dává státům právní nástroj na vyžadování standardů ochrany osobních dat. Trend vzrůstajícího počtu odcizených identit je neudržitelný. Se zdokonalováním ochrany se současně zdokonalují i útočníci, kteří tyto informace sbírají a zneužívají. Na tuto skutečnost narazila již nejedna velká nadnárodní společnost. Jednou z nejvíce medializovaných úniků osobních dat byla v roce 2019 kauza British Airways. Byla odcizena data 500.000 cestujících, kteří nakupovali a rezervovali letenky přes jejich online portál. Aerolinka byla shledána vinnou Evropskými autoritami, za nedostatečnou ochranu osobních dat svých klientů. British Airways byla vyměřena pokuta v hodnotě 1.5% celkového ročního výdělku aerolinky, což je 230 milionů dolarů. Závažnost tohoto problému poukazuje na nutnost změn při používání digitální identity jak pro zákazníka, tak pro zprostředkovatele služeb. [23]

Principem blockchainu je přístup k ochraně dat nazývajícím se „privacy by design“ (přirozené bezpečnosti dat). Ochrana dat je základní premisou, která do budoucna změní pohled na elektronickou identitu.

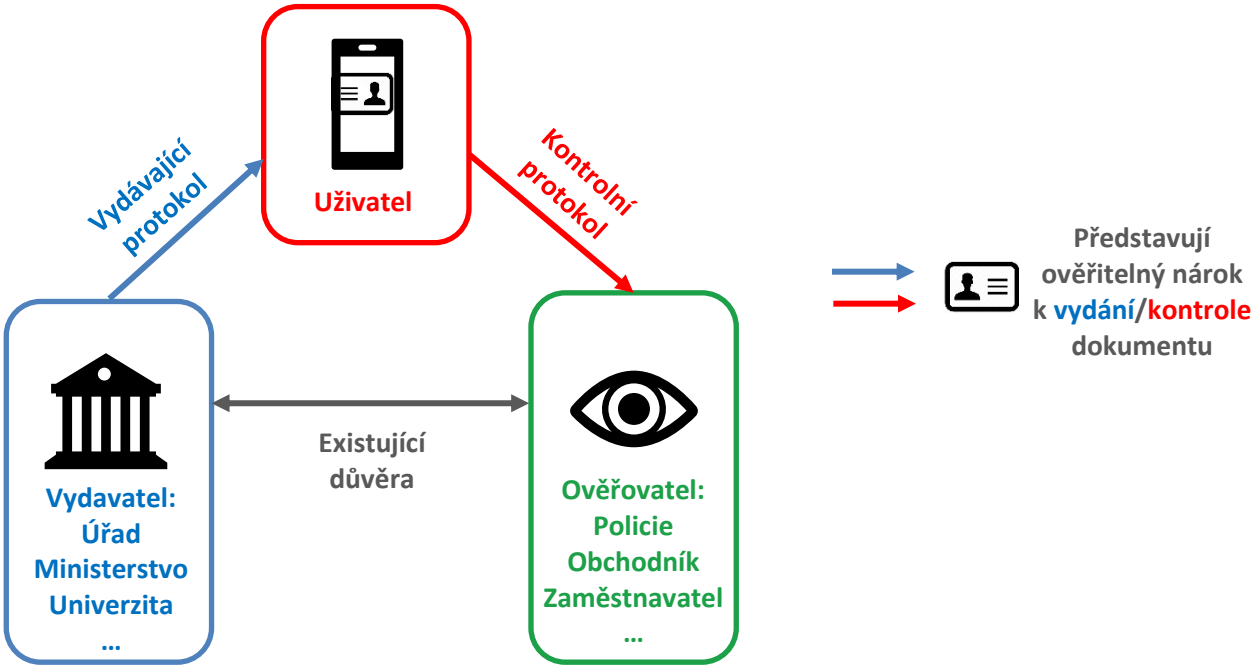
Nová technologie přinese mnoho změn do již zaběhnutých procesů. Proces ověřování identity cestujících v dnešní době funguje tak, že pomocí kombinace osobních dokladů a letenky

dostává cestující přístup do SRA (Safety Restrected Area) prostorů letiště. Dokumenty jsou kontrolovány buď za pomoci příslušníků bezpečnostních složek, nebo elektronicky pomocí automatických scannerů se čtečkami biometrických údajů. Dokumenty které bezpečnostní složky a čtečky kontrolují jsou uznávány minimálně ze dvou důvodů. Jejich formát je celosvětově standardizovaný. Druhým důvodem je důvěra ověřujících autorit, k autoritám které dokumenty vydávají. Tento ekvivalent ve virtuálním světě zatím neexistuje, avšak pomalu dozrává doba, kdy bude nutné začít s elektronickou identitou pracovat. V digitálním světě je počáteční a zároveň největší výzvou vytvořit ekvivalent cestovních dokladů, které budou plošně akceptovány jako důkaz identity. Pro ně bude nutné vytvořit infrastrukturu státních institucí a ověřovacích orgánů. Státní instituce budou muset vybudovat důvěryhodné cesty jak elektronické doklady standardizovat, aby ověřovací orgány mohly vyvinout postupy k efektivní kontrole. Další výzvou bude vydávání a následná využitelnost v ověřovacím procesu. Elektronická forma by následně za pomoci jednoduchých Wallet aplikací mohla sloužit k uchovávání privátních a veřejných klíčů. Klíče by tak byly využívány pro zjednodušenou komunikaci s autoritami, nebo se složkami zastupujícími autority. Vydávání a ověřování by mohlo probíhat pomocí ověřitelných nároků. Nároky by zajišťovaly vydávání certifikátů uživatelům a zároveň by umožňovaly ověřovacím autoritám žádat o přístup k digitálním dokumentům.

10.1 Ověřitelný nárok

Ověřitelný nárok by byl standardní definicí vyměňování a ověřování osobních dat. Nárok by záležel na úrovni důvěry mezi vydavatelem digitální identity a ověřovatelem identity, stejně jako to je ve fyzickém světě. Uživatel by vznesl ověřitelný nárok na získání elektronického dokladu. Vydávající entita by zkontrolovala jeho nárok a na jeho základě by přes vydávající protokol zajistila dodání dokladu uživateli. Stejně tak, pokud by kontrolní entita vznesla ověřitelný nárok k uživateli, tak by uživatel, přes kontrolní protokol mohl doklad předložit. Již fungující analogie je online nákup placený kreditní kartou. Obchodník se dotáže banky, zda má kupující dostatek financí na účtu. Banka zkontroluje obchodníka, zda je důvěryhodný a následně zkontroluje účet kupujícího. Pokud disponuje dostatkem financí, jsou peníze z účtu vyblokovány. V dalším kroku banka peníze z účtu klienta převede na účet obchodníka. V blockchainu je celý proces zjednodušen. Prodávající zažádá o platbu kupujícího. Kupující platbu pomocí aplikace Wallet provede a převede finance na účet obchodníka. Celý proces není kontrolovaný centralizovaným systémem banky, je automaticky kontrolovaný sítí. Síť zaštítí důvěryhodnost obou stran a za pomoci kryptografie obchod vypořádá. Stejným způsobem by se dal vytvořit

ekosystém pro vydávání osobních dokladů a certifikátů. Díky rychlému a důvěryhodnému přesunu dat v rámci blockchainu, by bylo možné vytvořit celosvětový ekosystém institucí vydávající doklady, vlastníků dokladů a ověřovatelů, kteří by v reálném čase efektivně vyměňovali ověřitelné nároky a zajistili bezpečnou kontrolu identity. Na obrázku je zobrazen diagram komunikace mezi stranami účastnícími se výdeje a kontroly elektronické identity. Uživatel získá, pomocí vydávajícího protokolu, například žádostí přes veřejný klíč autority certifikát, který si uloží do své aplikace Wallet. Certifikát je potvrzený, od oficiální autority, například od Ministerstva vnitra ČR, tím nabývá reálné hodnoty. Ve chvíli, kdy uživatel musí prokázat svojí identitu, například při oficiální komunikaci s Policií ČR, je pomocí kontrolního protokolu zažádán o přístup ke svému občanskému průkazu. Uživatel může v aplikaci Wallet zpřístupnit Policii ČR přístup ke svým identifikačním dokladům. Policie ČR po získání přístupu zkontroluje, zda byl dokument vydán oficiální autoritou. Protože Policie ČR uznává Ministerstvo vnitra jako důvěryhodného vydavatele dokladů, může důvěřovat i elektronické identitě uživatele.[24]

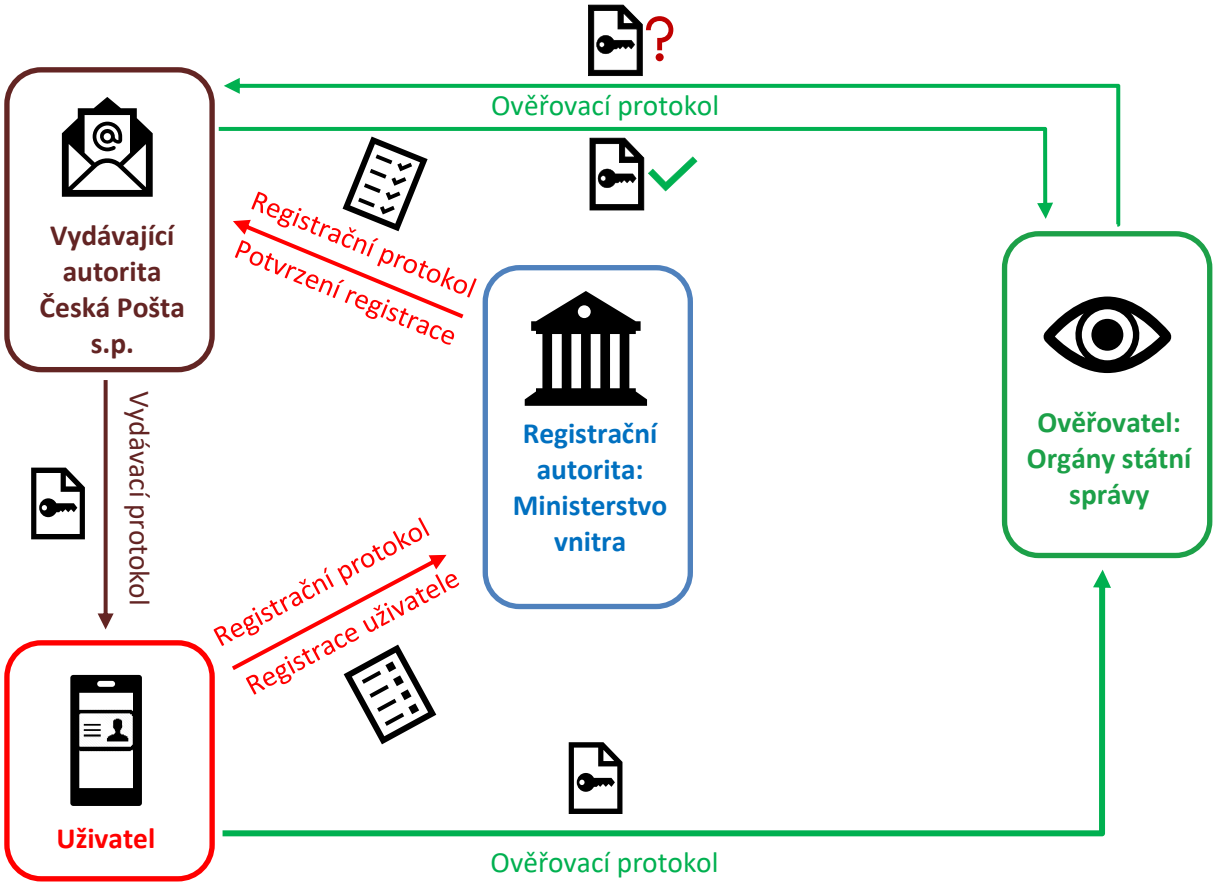


Obrázek 20 Ekosystém ověřitelných nároků [Autor]

10.2 PKI a DPKI

Jeden z již existujících způsobů ověřování identity je takzvané PKI (Public Key Infrastructure). Technologie se používá na zabezpečené přenosy citlivých dat, nebo například na podávání žádostí na úřad. Příkladem využití v ČR je datová schránka. Pro registraci do systému se musí žadatel zaregistrovat na stránce zřízené Ministerstvem vnitra. Následně je vytvořen účet. Údaje

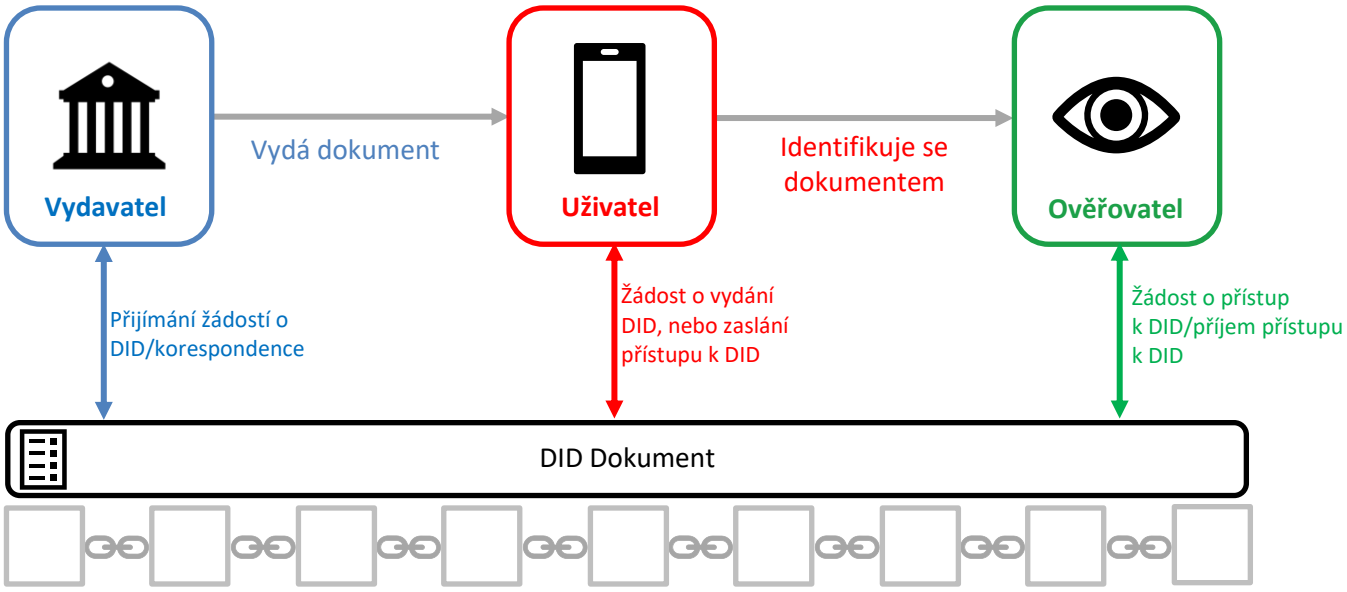
k účtu, zašle pomocí provozovatele (Česká Pošta s.p.), datových schránek uživateli. Občan následně může datovou schránku využívat ke komunikaci se státními subjekty, které jsou do sítě datových schránek připojeny. Česká Pošta funguje jako Certifikační subjekt a Ministerstvo vnitra jako Registrační subjekt. Zprávy jsou opatřeny časovým razítkem a zároveň jsou kryptograficky podepsány, takže je zde vysoká úroveň autenticity. Korespondence je dále uschovávána na serverech České Pošty, která se stará o jejich bezpečnost. Ověřovacím prvkem jsou všechny úřady, které s námi pomocí datové schránky komunikují. Soubor certifikátů, který Ministerstvo vnitra vydalo je průběžně aktualizován. Ověřovací autority, tak mohou mít jistotu, že jednají se správným subjektem. Tento systém je sice bezpečný, ale náročný na údržbu, centralizovaný a těžkopádný. [24]



Obrázek 21 Vizualizace PKI sítě [24]

Blockchain nabízí nový způsob řešení tohoto problému. nazývá se DPKI (Decentralised Public Key Infrastructure). DPKI nabízí možnost vynechat ze systému zprostředkovatele služeb, v příkladu Datové schránky, Českou Poštu. Data nebudou uložena na serverech

zprostředkovatele, ale budou v zakódované podobě uložena v rámci blockchainu. Přístup k datům bude mít pouze uživatel komu náleží, nebo komu uživatel dal přístup pomocí veřejného klíče příjemce. Základní ideou DPKI je vytvořit digitální identitu, kterou má pod absolutní kontrolou pouze její majitel. Identita by byla prokazována elektronickým certifikátem, který by byl vydáván oficiálním vydavatelem. Takovým vydavatelem by mohla být ministerstva, školy, úřady, nebo například ambasády. Základním kamenem DPKI je takzvaný Decentralized Identifier, zkráceně DID. DID je způsob který mohou využívat organizace i uživatelé k vytvoření unikátního kryptografického identifikátoru. Identifikátor je plně pod kontrolou vlastníka digitální identity a na rozdíl od doménového jména, IP adresy, nebo telefonního čísla, DID není zprostředkován třetí stranou, ale je vytvořeno samotným uživatelem a je uloženo v DID dokumentu. DID dokument tak slouží v rámci blockchainové sítě jako kniha adresátů, identita, které mohou vydávající autority vydat certifikáty s osobními doklady. Na základě DID by tak bylo možné vytvořit oficiální kanál na přímou komunikaci s úřady, bez nutnosti prostředníka. Ověřovací autority budou také vlastnit své DID. Uživatelé tak budou moci komunikovat a vydávat své osobní údaje ověřovacím autoritám, na základě jejich veřejného klíče.[24]



Obrázek 22 Implementace DID na Blockchain [24]

11 Správa digitální identity pro posádky

Další oblastí, ve které by mohl blockchain pomoci, je oblast licencování posádek. V dnešní době je stále nejčastějším způsobem zápisu letů do leteckého deníku v papírové podobě. Na trhu existují zápisníky letů v elektronické podobě, ale jedná se vlastně pouze o zálohování papírové podoby. Za oficiální dokument je stále považovaný pouze fyzický zápisník letů. S fyzickým zápisníkem letů je však spojeno spíše více nevýhod, než výhod. To samé platí o licencích, které jsou vydávány pouze ve fyzické podobě. Pokud se tedy tyto doklady ztratí, nebo jsou odcizeny, může dojít odcizení identity vysoce specializovanému personálu. To může znamenat velkou hrozbu pro osoby a majetek nejen přepravované v letadle, ale i na zemi. Dále se tak může snížit možnost zapomenutí dokladů doma, což může pro pilotům i aerolinkám ušetřit mnoho nepříjemností.

11.1 Licencování posádek

Velký potenciál skýtá blockchain také pro evidenci a obnovování licencí posádek. Stejně jako může blockchain pomoci zmodernizovat identifikaci osob, může posunout těžkopádný způsob licencování posádek. Blockchain může pomoci standardizovat a automatizovat mnohé procesy spojené s vydáváním, správou leteckých a zdravotních ověření způsobilosti. Jeho transparentnost umožňuje vydávajícím autoritám komunikovat a schvalovat žádosti o průkazy pomocí Smart kontraktů, vydávat licence pomocí certifikátů, které budou snadno propojitelné s chytrými telefony, nebo jinou výpočetní technikou. Kontroly SAFA (Safety Assessment of Foreign Aircraft) budou moci probíhat efektivněji, tím se zamezí zbytečným zdržením a problémům s chybějícími fyzickým dokumenty.

11.1.1 Organizace

V síti by figurovaly tři základní entity. Vydávající autority, ověřovací autority a uživatelé. Vydávající autority zastupují Úřady civilního letectví, Ústavy leteckého zdravotnictví a schválení letečtí examinátoři. Uživatelé by na základě registrace žádali vydávající autority o vydání jejich DID. Zapsáním DID do DID dokumentu by byl se nastaven komunikační kanál mezi uživatelem, ověřovatelem a vydávající autoritou. Pomocí žádosti přes veřejný klíč by následně uživatelé žádali autority o vydání elektronických průkazů způsobilosti. Průkazy způsobilosti by následně byly vydávány za pomoci veřejného klíče uživateli ve formě certifikátu. Tento certifikát by byl uložen aplikaci Wallet, ze které by bylo možné tyto informace spravovat a sdílet. Ověřovací autority by mohly uživatele žádat o zpřístupnění jejich dat. Výhoda tohoto systému spočívá

v absolutní kontrole uživatele nad sdílenými informacemi, může si například vybrat, že bude sdílet pouze získané kvalifikace, ale nebude sdílet své pohlaví, či národnost. Zároveň posílá data v zakódované podobě, kterou může přečíst pouze adresát. Ověřovací autorita se tak dále nevystavuje nebezpečí odcizení poskytnutých dat, protože kontrola může probíhat naprosto automaticky bez nutnosti člověka. Ověřovací autority letecké způsobilosti by dle potřeby byly například vykonavatelé kontrol SAFA, letecké společnosti, letecké školy, examinátoři, nebo například obchodníci, kteří na základě licencí mohou vydávat zvýhodněné ceny svých produktů.

11.1.2 Technická stránka a metody komunikace

Základní ideou je vytvořit důvěryhodný vztah mezi vydávající autoritou a kontrolní autoritou. Pokud si tyto dvě entity bezvýhradně důvěřují může nám blockchain pomoci vytvořit elektronickou identitu, která může být následně považována za oficiální elektronický dokument. Vydávající autority vytvoří celosvětový standard jak má elektronická licence vypadat, aby splňovala všechny parametry ICAO a tím pádem jí mohly ověřovací využívat, jako zdroj pravdivých informací. Nejvýhodnějším typem architektury pro tvorbu mezinárodního leteckého blockchainu je hybridní blockchain. Mezinárodní spolupráce by probíhala v rámci veřejné vrstvy blockchainu a vnitrostátní by probíhala na samostatných privátních, či veřejných blockchainech. Vnitrostátní, privátní blockchainy by musely využívat různě škálovaný přístup. Škálování by zajistilo rozdělit různé pravomoci a funkce zúčastněným stranám. Tak by bylo možné dát úřadům pravomoc zasahovat do funkce své privátní sítě a tak udržet její správné fungování. Bloky by byly uzavírány vydávajícími autoritami. Mechanizmus konsensu by bylo vhodné využít cokoliv co podporuje platforma, kterou si tvůrci sítě zvolili. Po uzavření bloku by byly nové bloky distribuovány ostatním vlastníkům plné kopie blockchainu. Plné kopie blockchainu by bylo vhodné skladovat na serverech vydávajících autorit. Zmenšené kopie blockchainu by byly distribuovány všem uzlům sítě. Skladováním plných kopií blockchainu pouze u vydávajících autorit, které mají nad uzavíráním dat kontrolu zabráníme možnosti pokusů o manipulaci se sítí, ze strany uživatelů, jež jsou jediní, co mohou manipulací dat získat výhodu.

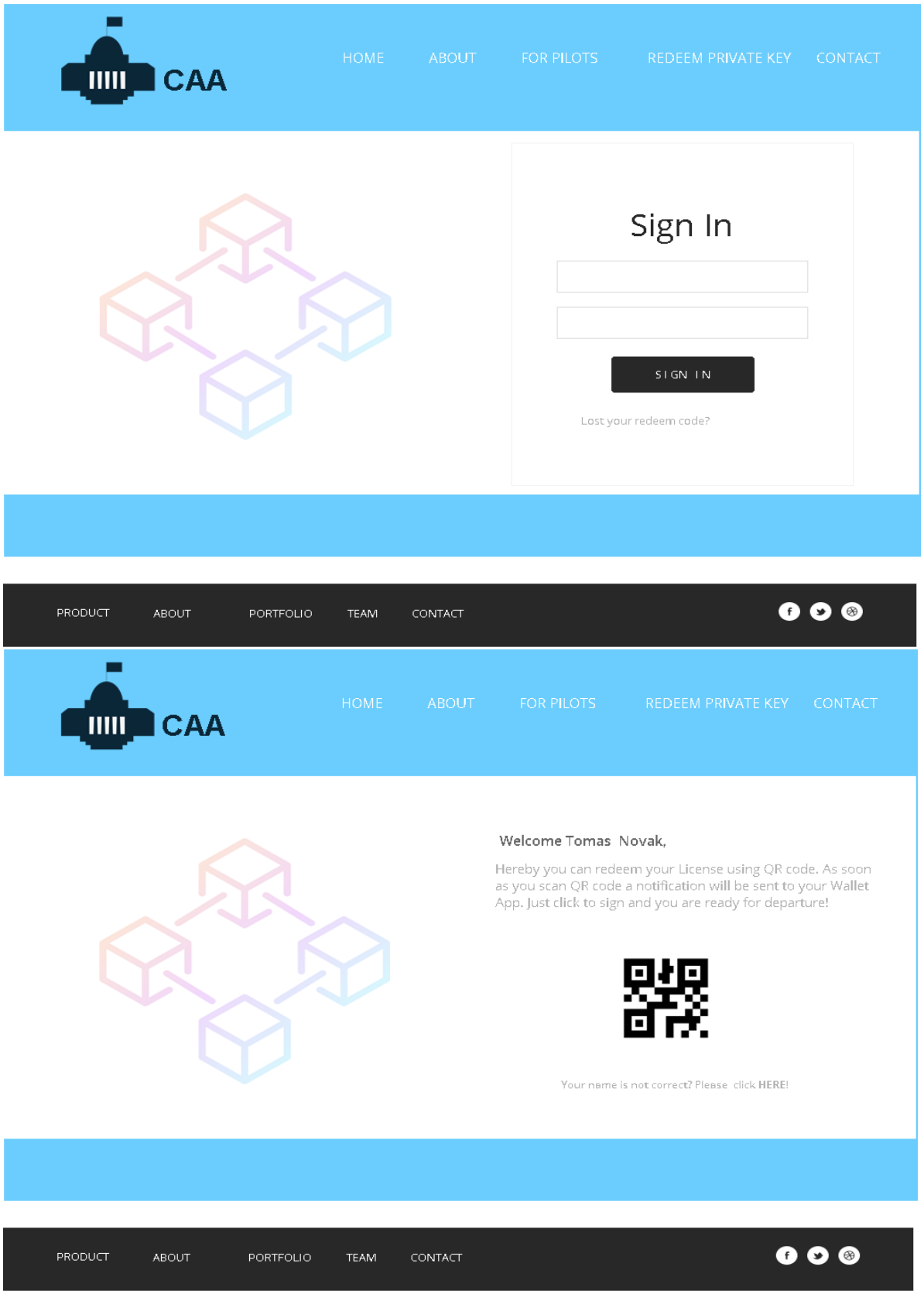
Hyperledger Sawtooth, Fabric i hybridní blockchain Polkadot nabízí možnost přidat k blockchainu další aplikace, které by mohly tuto síť podpořit. DID Dokument by mohl pomoci adresováním oficiálních žádostí pilotů, úřadů i aerolinek. Oficiální mezinárodní kanál pro komunikaci s leteckými úřady by dále mohl pomoci zúčastněným sjednotit, zabezpečit a zefektivnit průběh komunikace, například při změně vydávajícího státu licence. Certifikáty

vydávané pomocí DID protokolu by bylo nutné vydávat s určitou dobou platností. Platnost by bylo možné vytvořit pomocí Smart kontraktu. Smart kontrakt by byl nastavený na určitý čas. Jakmile by se doba expirace Smart kontraktu přiblížila, uživatel by byl upozorněn notifikací. Zároveň by mu tak bylo možné nabídnout možnost prodloužení, či obnovy certifikátu. S tím by byl spojený vznik nových typů žádostí, které by byly zcela digitalizované. Digitalizované žádosti mají výhodu intuitivních nabídek ke správnému vyplnění, které by ulehčili práci jak uživateli, tak samotným úřadům.

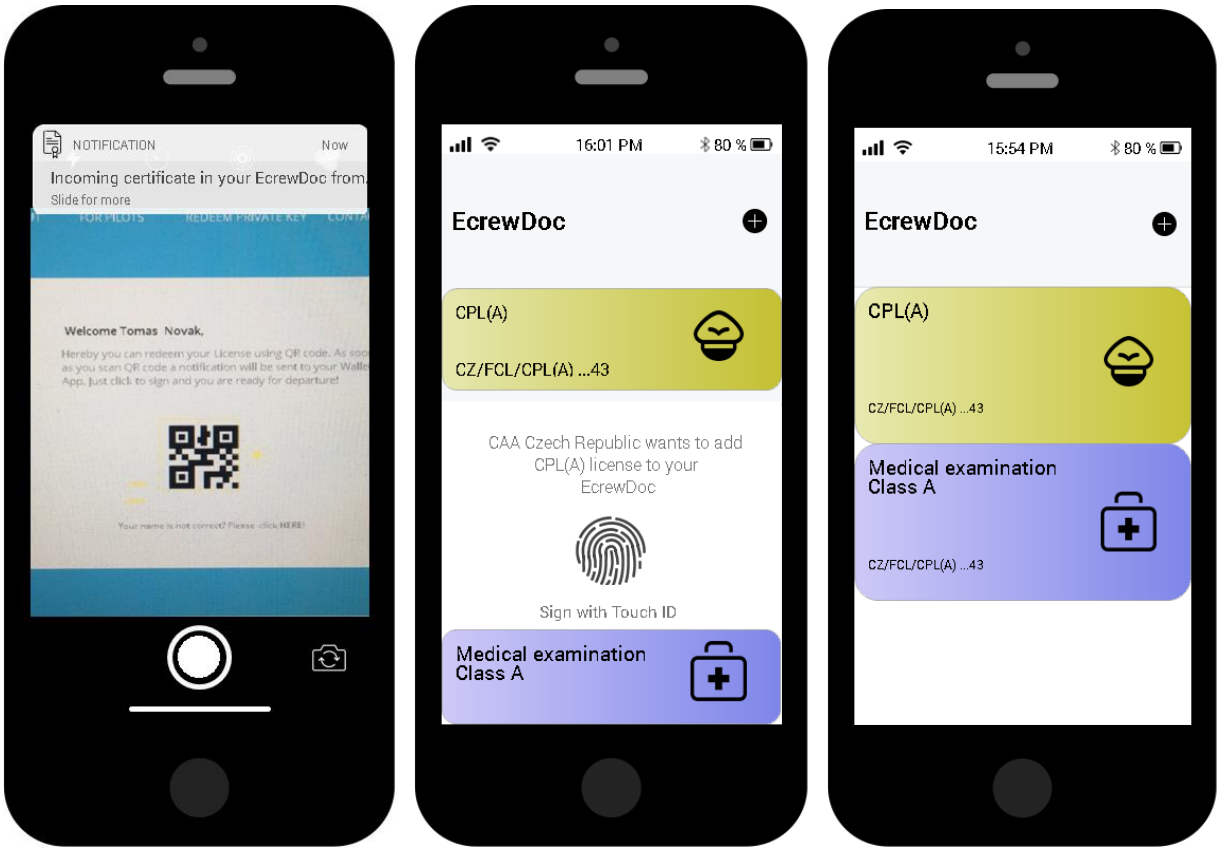
11.1.3 Uživatelské rozhraní

Uživatelské prostředí musí být navrženo intuitivně a jednoduše. Všechny zúčastněné strany musí své požadavky zadávat efektivně a v reálném čase. Aplikace Wallet musí být spustitelná na naprosté většině zařízení. Proto je nutné ji naprogramovat v multiplatformním rozhraní. Multiplatformní rozhraní zvýší použitelnost aplikace a radikálně sníží cenu za tvorbu a následnou údržbu sítě.

Základní problematikou je přidání licence do zařízení uživatele. Licence je do aplikace Wallet nutné uložit jako druh certifikátu, který by byl vydáván na základě informací zapsaných v blockchainu. Proces vydání certifikátu by začal vytvořením DID uživatele. Uživatel by si registrací vytvořil účet, který by byl přidán do DID dokumentu sítě. S tímto identifikátorem, by se uživatel prokázal vydávající autoritě. Vydávající úřad by uživateli vygeneroval jednorázové přístupové informace, ve formě uživatelského jména a hesla. Jakmile by získal přístupové informace mohl by se na stránkách vydávající autority přihlásit. Po přihlášení k webovému rozhraní se zobrazí základní informace o pilotovi spolu s QR kódem. Uživatel pomocí QR kódu zašle požadavek k zaslání certifikátu. Certifikát se automaticky přidá do aplikace Wallet. Od této chvíle by uživatel mohl uživatel využívat tuto elektronickou identitu a využívat výhody sítě.



Obrázek 23 Vyzvednutí DID na fiktivním portálu Úřadu civilního letectví [Autor]



Obrázek 24 Vizualizace aplikace Wallet pro účely posádek [Autor]

11.1.4 Výhody

Využití decentralizované sítě pro skladování informací je nutný krok pro další vývoj letectví. Systémy vydávání způsobilostí jsou zastaralé a nekompatibilní s moderním světem. Je nutné vytvořit nový bezpečný protokol pro správu osobních dat. Internet změnil vnímání světa, proto je nutné se přizpůsobit jeho plnému potenciálu. To však nebude možné do té doby, než z něj vytvoříme důvěryhodné prostředí.

Základní výhodou pro uživatele musí být jednoduchá a bezpečná správa informací. Systém bude využívaný pouze ve chvíli, kdy je vytvořeno intuitivní prostředí. Fungující implementace správy elektronické identifikace jsou založeny na PKI, které je těžkopádné a náročné na údržbu. Proto je ideální tvorba DPKI sítí, které budou fungovat na blockchainových principech.

Vytvořením elektronické identity pilota, uživatelé získají bezpečný kanál, ve kterém bude možné jednoduše sdílet data. Piloti získají možnost komunikovat s úřady, aerolinkami, nebo například obchodníky pomocí svých DID a certifikátů.

Piloti získají možnost žádat o práci pomocí aplikace Wallet. Nabídky práce budou obsahovat QR kód, který po naskenování automaticky vygeneruje funkci na poskytnutí dat zaměstnavateli. Aplikace automaticky vyplní veřejný klíč adresáta a veřejný klíč odesílatele. Uživatel následně vybere data, která je ochoten sdílet a potvrdí odeslání. Potvrzení zaslání dat bude moci probíhat pomocí hesla, nebo pomocí FaceID, popřípadě TouchID. Adresát tak získá cílené informace o žadateli o práci. Takto vzniklý informační kanál je velice odolný na únik dat a obě strany tím chrání své zájmy. Uživatel může sám rozhodovat o tom jaká data budoucímu zaměstnavateli odešle. První kola výběrových řízení tak mohou probíhat částečně anonymně a můžeme systémově zabránit rasové, nebo genderové diskriminaci, nebo naopak protežování účastníků na základě známostí. Použitím Smart kontraktu by bylo možné nastavit automatické odeslání informací o dalších krocích výběrového řízení. Takto by se eliminoval lidský faktor HR oddělení, které je v období náboru zahlceno stovkami žádostí o práci. Pokud se podaří vytvořit správný formát uchovávání dat, může tak pilot těžit i z podstaty digitálních dat. Bylo by možné vytvořit digitální formuláře na prodlužování a vydávání průkazů, které by z části bylo možné vyplňovat automaticky pomocí aplikací Wallet. Pokud by pilot potřeboval řešit problém s úřadem pro civilní letectví své, nebo jiné země, bylo by možné navázat přímé důvěryhodné spojení přenosů dat pilota, bez porušování GDPR, nebo zdlouhavého a finančně náročného zasílání informací mezi úřady v papírové formě. Nyní, pokud chce pilot zažádat o validaci leteckého průkazu a jeho vydání jinou zemí, musí kontaktovat Úřad pro civilní letectví ve své zemi, která zajistí zaslání dokumentace cílové zemi. Zároveň požádat AME o zaslání žadatelovi dokumentace oběma autoritám civilního letectví. Všechna tato komunikace probíhá v papírové formě, případně za pomoci emailové korespondence. Což představuje z hlediska ochrany osobních dat nebezpečné prostředí pro obě strany. Jedná se zároveň o zbytečně robustní a neefektivní způsob. Ve stále měnícím se prostředí letectví mohou tyto časové proluky mohou znamenat pro aerolinky i pro piloty problém. Neefektivní komunikace může znamenat pro pilota velké finanční a profesní problémy. Pokud by uživatel v blockchainové síti žádal přenos dat mezi úřady, pouze by pomocí veřejného klíče nalezeného v DID dokumentu zaslal žádost současnému a budoucímu úřadu. Další výhodou by pro pilota byla možnost získávat výhody při koupi materiálu nutného pro vykonávání práce. Například firma BOSE nabízí slevy na letecká sluchátka pro komerční piloty. Piloti jsou však odevzdávat citlivá data firmě, která může být kdykoliv napadena hackerským útokem. Přitom by prodejci stačilo pouze potvrdit, zda kupující pilotní průkaz vlastní. Prodávající by proto nemusel žádat zákazníka o číslo licence. Pouze by vytvořil požadavek pomocí veřejného klíče o informaci, zda zákazník vlastní licenci. Zákazník tak není vystaven riziku ohrožení svých osobních dat a obchodník

nemusí data dále zabezpečovat, aby naplnil požadavky GDPR. Letecké autority v rychle se měnícím světě začínají působit velmi těžkopádným dojmem. Jedním důvodem tohoto stavu je exponenciální nárůst provozu. Dalším důvodem je náročné přizpůsobování se zrychlující době. Protože je nutné zajistit vysokou míru bezpečí, každá změna je aplikována ve chvíli, kdy přestává být aktuální. Proto je nutné základní procesy automatizovat a co nejvíce zjednodušit. Jakmile se zefektivní základní procesy v komunikaci s úřady, examinátory a letecko-zdravotnickými centry vznikne potenciál pro rozvoj. Energie ztracená v byrokratických úkonech, se dá nasměrovat k udržení kroku s rychle se měnícím světem. Vzdělaný a nedostatkový personál by se mohl zabývat problematikou, která odpovídá jeho kvalifikaci. Další obrovskou zátěží je udržení bezpečného prostředí v oboru osobních údajů. Tyto investice by mohly s používáním blockchainu odpadnout a mohly by nadále sloužit k dalšímu rozvoji vlastního civilního letectví. Pro autority by byl jednoduchý oficiální komunikační kanál mezi sebou navzájem, aerolinkami, nebo piloty. Do blockchain se dají nadále implementovat aplikace pro zabezpečenou komunikaci. Adresování pomocí DID Dokumentu a veřejným klíčům by tak mohlo pomoci podávání žádostí online. Úřad by tak mohl systém žádostí plně automatizovat a mohl by se soustředit pouze na sporné případy a urychlit tak jejich řešení. Aerolinky by v případě využití elektronických leteckých licencí získaly důvěryhodný a jednoduchý způsob, jak rekrutovat nové piloty do svých řad. Jednoduchý a efektivní způsob by napomohl transparentnosti při výběrových řízeních. Automatizováním příjmu přihlášek by firmám snížila zátěž na personální oddělení, která musí v období výběrových řízeních spravovat stovky konverzací najednou. Chytrou implementací aplikací zjednodušujících základní konverzaci, by bylo zabráněno omylům a možným pokusům o podvodné chování. Tím, že blockchain pro správu identity je ze své podstaty důvěryhodný zdroj, nemusely by aerolinky být vystaveny nebezpečí rekrutování nedostatečně certifikovaného personálu. Komunikace s autoritami by následně byla zajištěna pomocí zabezpečeného komunikačního kanálu. Zabezpečený kanál by mohl sloužit i pro odesílání dokumentace pro prodloužení kvalifikací pilotů. Examinátoři by mohly ihned po ukončení zkoušky za pomoci aplikace Wallet, jednoduše a bez prodlení informovat o prodloužení kvalifikace personálu. Transparentnost by také mohla pomoci aerolinkám dělat průzkumy trhu. V DID dokumentu by vyhledala adresy uživatelů, kteří vlastní potřebné kvalifikace a pomocí dotazníku by bylo možné zjistit, jaké má aerolinka možnosti na zaplnění pilotních pozic. Firmám dále odpadne nutnost skladovat citlivá data na svých serverech a tím se zabezpečí proti porušení GDPR a následným možným pokutám.

11.2 Zápisník letů

Zápisník letů je pro každého pilota velice důležitý dokument. V zápisníku letů pilota jsou zapsány informace o provedených letech od začátku výcviku. Valná většina leteckých deníků je standardizována tak, aby splňovala nároky organizace ICAO. Zaznamenává se do něj den, čas odletu, místo odletu, čas příletu a místo příletu. Dále je v něm zaznamenáno v jakých podmínkách byl let vykonán, IFR, nebo VFR. Typ a registrace letounu využitého pro let, jaká posádka a jaké byly jejich funkce. U pilota se často jedná o jediný dokument prokazující míru jeho zkušenosti. Kvůli jeho vysoké důležitosti je považován za základní zdroj informací pro žádost o vydání licence, nebo při výběrových řízeních na pilotské pozice. Z toho důvodu je nutné, aby byl deník pravdivým a transparentním zdrojem informací.

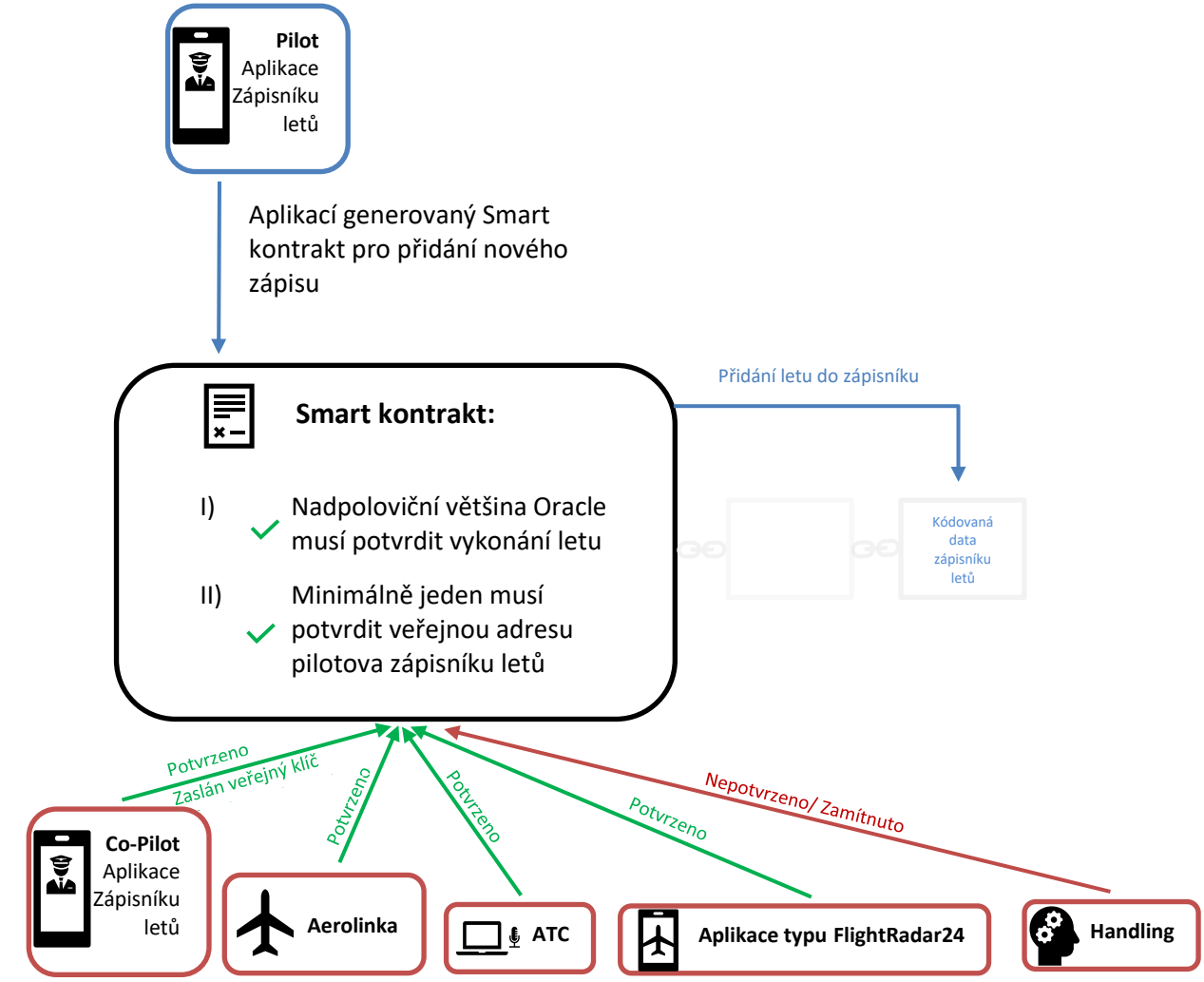
Tím, že se u mnoha pilotů jedná o jediný zdroj informací o vykonaných letech, je zde vysoké nebezpečí ztráty, nebo odcizení. Proto s příchodem osobních počítačů a inteligentních zařízení vzniklo mnoho aplikací, umožňujících digitalizaci těchto dat. Digitalizací zápisníku letů vzniká lépe strukturalizovaný zápis. Tato strukturalizace umožňuje lepší přehled nalétaných hodin, možnost exportovat data do různých formátů a s tím možnost zálohovat data. Avšak pokud si pilot vede pouze elektronický zápisník letů je veliká pravděpodobnost, že bude vystaven situaci, kdy nebude považován za důvěryhodný. Důvěryhodnost papírového zápisníku letů spočívá v přítomnosti podpisů vlastníka, razítek a podpisů úřadů, examinátorů a instruktorů. Blockchain by mohl přinést mnoho výhod i do tvorby věrohodných elektronických zápisníků letů. Zápisníky bude možné distribuovat v síti a za pomoci asymetrické kryptografie sdílet a podepisovat úřady, examinátory, nebo leteckými společnostmi.

11.2.1 Síť, uživatelé a zapojené organizace

Bylo by výhodné, kdyby zápisník letů byl spojen se sítí na správu elektronických licencí. Získala by se tak celistvost systému, kde by letecký průmysl získal globální kontrolu nad výcvikem, zkušenostmi a certifikací pilotů. Z transparentního a globálního přístupu k datům, by mohly těžit aerolinky, letecké školy, letecké úřady, organizace pro civilní letectví a zároveň i piloti a cestující. Aerolinky by získali oficiální nástroj pro správu náletů svých pilotů a zároveň by mohly pomocí filtrů zjistit počet pilotů, kteří jsou právě ve výcviku a se kterými mohou do budoucna počítat. Zároveň mohou získat důvěru, že data poskytnutá v leteckých zápisnících jsou pravdivá. Letecké úřady by poprvé v historii měly globálně ucelený obrázek o náletech pilotů. Mohly by tak provádět účinnější kontroly a zajistit dodržování norem. Piloti by získali jednoduchý nástroj na správu svých zápisníků letů a zároveň oficiální kanál na komunikaci

s úřady, například při žádosti o prodloužení svých způsobilostí. Nejvíce by ze systému samozřejmě těžili cestující, kteří by si mohli být jisti, že letoun je operován plně vycvičenou posádkou.

Jednalo by se tedy o privátní síť, nebo hybridní síť, kde by uživatelé nebyli anonymní. Architektura vhodná pro tuto nástavbu by byla stejně jako u databáze pro správu elektronických licencí, Hyperledger Sawtooth, nebo Hyperledger Fabric, Iroha nebo hybridní síť Polkadot. Informace o vykonaných letech by byly zapisovány samotnými piloty. Důvěryhodnost těchto informací by byly potvrzovány sítí softwarových Oracle. Za Oracle by byly využívány informace od organizací, jako je řízení letového provozu, letečtí dopravci, aplikace typu Flightradar24 a zároveň piloti sami mezi sebou, nebo například cestující. Vícenásobné potvrzování informací, zvýší důvěryhodnost vložených dat. Zároveň by zde data byla bezpečně uložena, automaticky aktualizována a jednoduše filtrována. Základní funkcí pro přidání letu do blockchainu by byl Smart kontrakt. Smart kontrakt by byl manuálně, nebo automaticky vyplněn do aplikace. Následně by byl vystaven síti softwarových Oraclů. Ty by na základě kritérií vyhodnotily správnost zapsaných údajů a zápis označili za důvěryhodný, nebo nedůvěryhodný. Následně by data byla přidána do blockchainu. Na vizualizaci níže uživatel vyplní informace o provedení letu do aplikace elektronického zápisníku letů. Aplikace vytvoří Smart kontrakt, který je vystaven kontrole. Kontrola probíhá za pomocí externích zdrojů informací, Oraclů. Jakmile více než polovina zdrojů potvrdí, že let byl vykonán a jeden zdroj potvrdí i veřejnou adresu jednoho z uživatelů, je možné let považovat za důvěryhodný. Potom jsou tato data přenesena do blockchainu, kde k němu má za pomoci své aplikace s privátním klíčem uživatel.

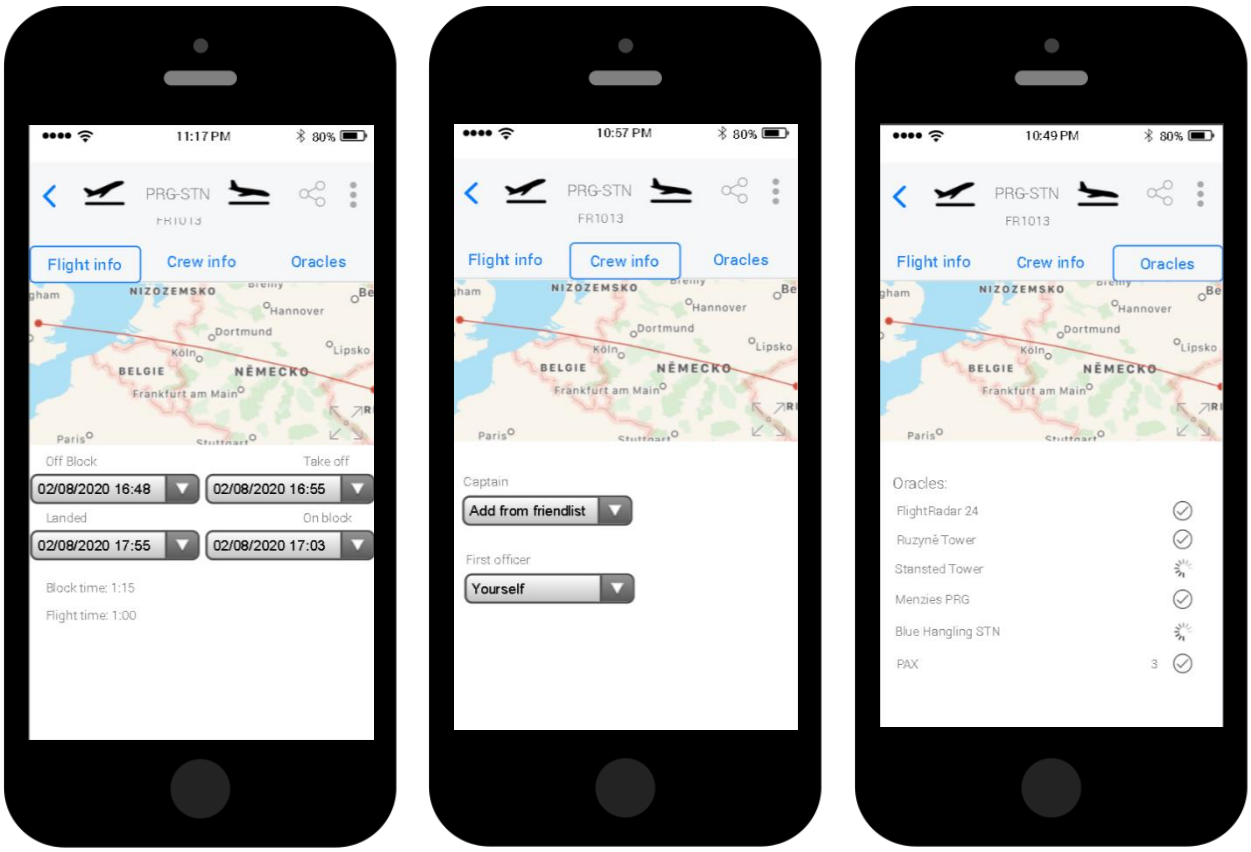


Obrázek 25 Přidání záznamu do zápisníku letů [Autor]

11.2.2 Uživatelské rozhraní

Vedení elektronického a zároveň papírového zápisníku letů, je ukázka neefektivního způsobu využívání moderní technologie. Za pomoci blockchainu je možné vytvořit elektronický zápisník letů, kde jsou důvěryhodná data zapisována do boků a distribuována celé síti. Elektronický zápisník letů v sobě kombinuje prvky aplikace Wallet (uchovává veřejný a privátní klíč), zároveň však prostředí pro zápis údajů, které následně vytvoří Smart kontrakt. Zápis těchto údajů musí strukturu schváleného ICAO zápisníku letů. Pokud by byl elektronický zápisník letů součástí systému s elektronickou identitou pilotů, bylo by možné tuto funkci implementovat do jedné aplikace. Tím pádem by vznikl univerzální nástroj pro správu kvalifikací.

Přidávání letů by bylo možné řešit více způsoby. Základní způsob by spočíval ve vyplnění informací ručně. Uživatel by zadal typ a registraci letounu, které si je možné uložit jako šablonu. Dále by musel vyplnit letiště odletu, destinaci, podmínky letu a posádku. Druhý způsob zápisu do leteckého deníku by fungovala automatickým způsobem. Pilot by vybral číslo letu, jméno kapitána a v čas opouštění bloku, by zahájil zápis. V čase příjezdu do bloku, by byl zápis ukončen. Zbylé informace by byly automaticky vyplněny pomocí veřejně dostupných informací z ADS-B. Ukončením zápisu by spustilo potvrzovací proces. Třetím způsobem by mohlo být pomocí scanu QR kódu. Některé aerolinky po skončení letu zasílají pilotům potvrzení o vykonaném letu. Jakmile piloti po letu vyplní Elektronický zápis letu, jsou tato data odevzdána operačnímu oddělení ke kontrole. Jakmile proběhne kontrola, je zaslán pilotům email s potvrzením vykonaného letu. Součástí potvrzení by mohl být QR kód, který by pilot pomocí mobilního fotoaparátu přečetl. Jakmile by byl let do aplikace vyplněn, aplikace by data vystavila kontrolnímu proces. Následně by data byla automaticky by byl uložena jako potvrzená, nebo naopak nepotvrzená. Postupem času, by bylo možné se zbavit zadávání jména kapitána a vypisování časů. Pilot by mohl do aplikace stáhnout svůj roster. Let by se automaticky zaznamenal pomocí externích informací od handlingových společností, letecké společnosti a dalších potvrzovatelů informací. Po skončení letu, by se aplikace uživatele požádala o potvrzení pravdivosti údajů. Jakmile by uživatel pomocí využití hesla, nebo biometrických údajů let potvrdil, byl by automaticky zapsán do řetězce.

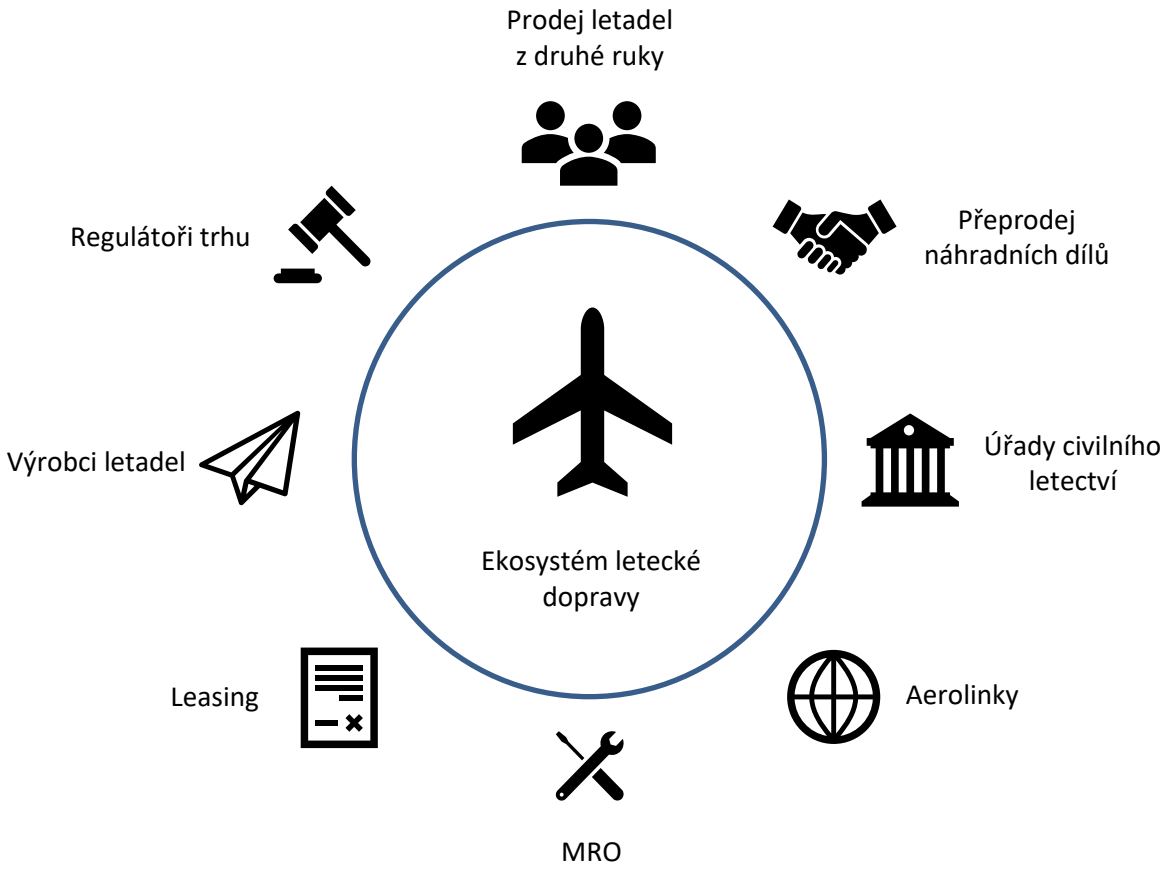


Obrázek 26 Vizualizace zápisu a kontroly letu

Tento koncept však musí počítat i s možností zaznamenat data z minulosti a nějakým způsobem vyřešit problém, kdy Oracle nebudou moci potvrdit vykonaný let. Jednalo by se hlavně o lety s letouny, které nejsou vybaveny ADS-B, nebo VFR lety v prostorech bez řízení letového provozu. Aby systém mohl fungovat, je nutné zavést dva typy zápisu hodin. Na lety systémem potvrzené a nepotvrzené. Systém musí dovolovat zapsat data, která nesplnila podmínky důvěryhodného zápisu, avšak označí je za nepotvrzená. Nepotvrzené lety bude moci žadatel o práci, nebo průkazu podložit fyzickou podobou zápisníku letů. Postupem času bude možné předpokládat, že většina pilotů přejde z papírové verze do digitální a důvěryhodnost digitálně potvrzených letů se zvýší. Následně už bude pouze na zaměstnavatelích, který typ zápisů preferují a jak si nastaví podmínky náboru nových pilotů. Do aplikace bude možné přidat funkci vložení nepotvrzených letů z minulosti. Zadání je možné řešit manuálním zápisem, potažmo pomocí přenesení z jiné aplikace zápisníku letů, Excelové tabulky, nebo jiného druhu standardizovaného výstupu. Ze začátku, důvěryhodnost zápisníku letů pomocí technologie blockchain nebude vysoká. Avšak s narůstajícím počtem účastníků sítě by se důvěryhodnost systému výrazně zvýšila.

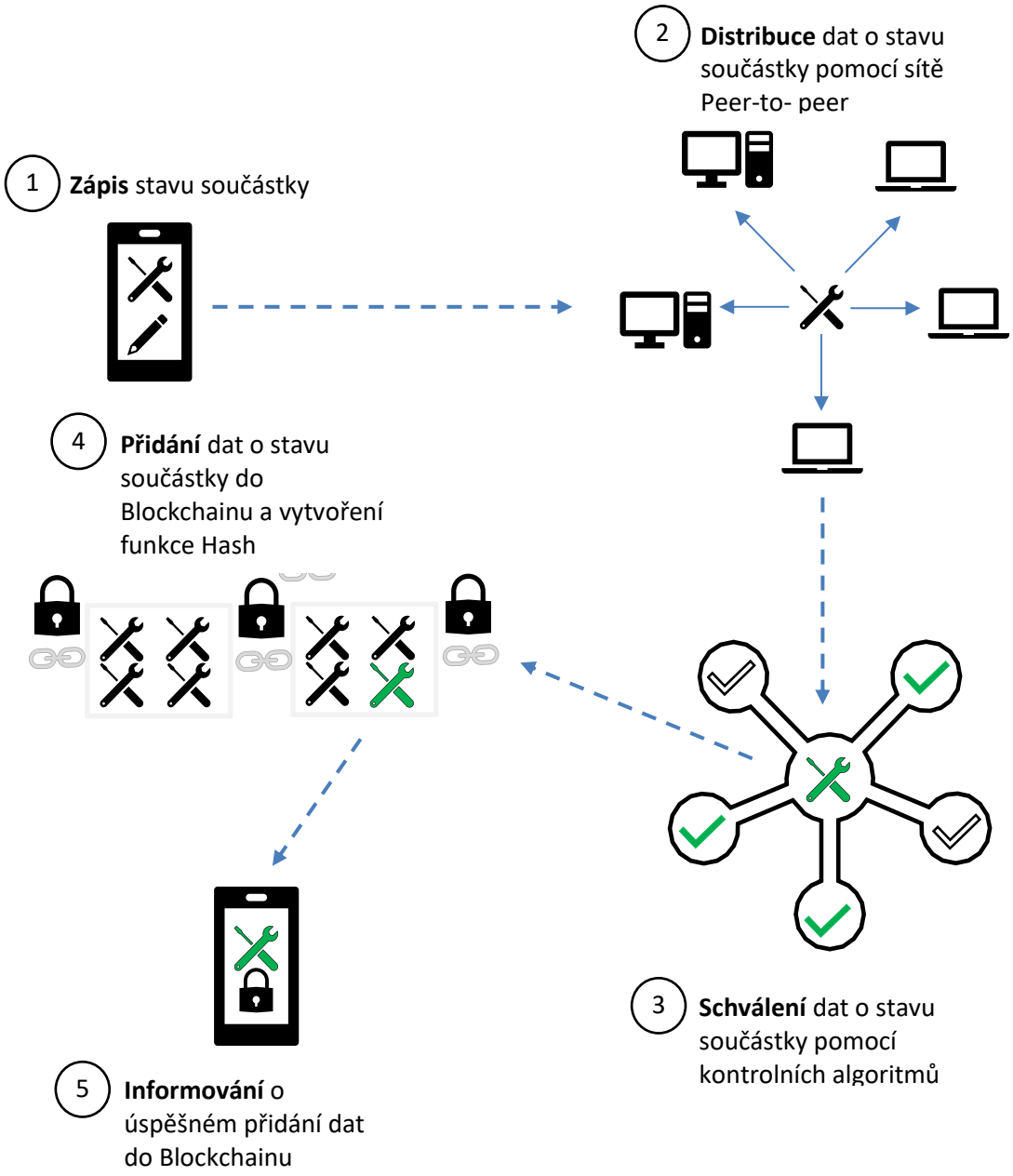
12 Kontrola technické způsobilosti

Přes všechen technologický pokrok, kterým letectví za více než století prošlo, je drtivá většina dat zajišťující letuschopnost, sbírána manuálně. Milióny životně důležitých součástek jsou kontrolovány za pomoci lidských smyslů. Po provedení kontroly jsou tyto informace ručně zaznamenávány do technických zápisníků. Technické zápisníky následně velmi často tvoří pro letecké mechaniky jediný informační zdroj o stavu letounu. Ti se často snaží udržet letky čítající desítky až stovky letounů bezpečně letuschopné. Do řetězce organizací zapojených do údržby letounů nejsou zařazeni pouze poskytovatelé MRO (Maintenance, repair and overhaul – Údržby, oprav a generálních oprav), ale zároveň i dodavatelských služeb a skladů. Všichni výše zmínění jsou povinni skladovat a udržovat informace o historii leteckých součástek. V případě, že je minulost součástky nejasná, musí být její letuschopnost vystavena zkouškám a opakované certifikaci. Drtivá většina dat, které jsou o letounech sbírány nemá svoji digitální podobu. John Maggiore, který je vedoucí údržby pro firmu Boeing tvrdí, že 90% technické dokumentace na světě je skladováno v papírové formě. Tím pádem se skutečně jedná o miliony krabic určených ke skladování životně důležité dokumentace. Tato skutečnost zapříčiňuje, neexistenci jednoduchého a důvěryhodného způsobu kontroly okamžité letuschopnosti, nebo letuschopnosti letounu v průběhu jeho provozování. Data jsou totiž šířena mezi více uzly komunikace, v různých formátech a následně izolována v samostatných systémech poskytovatelů služeb. Tím pádem data o součástkách letounů, které náleží do jednoho ekosystému dodavatelů, prodejců, aerolinek a dalších, nejsou a nemohou být sdíleny do všech stran stejným způsobem. Digitalizace zároveň řeší mnoho dílčích problémů, které skýtá papírová forma, jako je její náchylnost k poškození, náročnost na skladování, zálohování a hlavně efektivní hledání v historii jednoho letounu, nebo dokonce celé letky letounů.



Obrázek 27 Ekosystém letecké dopravy [25]

Nepřehledností, nedostupností a nedostatečnou transparentností vzniká velký potenciál pro manipulaci s historií a černý trh s částmi letadel. Blockchain i v tomto případě může sehrát významnou roli pro změnu standardů sběru, přechovávání a sdílení informací. Pomocí blockchainu je možné vytvořit něco jako rodný list každého dílu a následně provádět digitální záznamy po celou dobu jeho životnosti. Pokaždé, když bude součástka kontrolována, opravována, nebo nahrazována, bude mechanikova povinnost data zanést do systému a podepsat svým privátním klíčem. Díky tomu bude v historii zaznamenáno na jakém letounu je umístěna, její přesná lokace v letounu, jaký je její stav, kolik cyklů je v provozu a kdo a kdy provedl opravu a vypuštění do provozu. Blockchain takto trvale zaznamená neměnnou minulost v průběhu času. Důvěryhodnost a nutnost konsensu všech stran, tak může vtvořit jednotnou a přehlednou historii pro celý průmysl a současně umožnit její téměř okamžité posouzení kdekoliv na světě.



Obrázek 28 Vizualizace komunikace sítě [25]

12.1 Ekonomické výhody

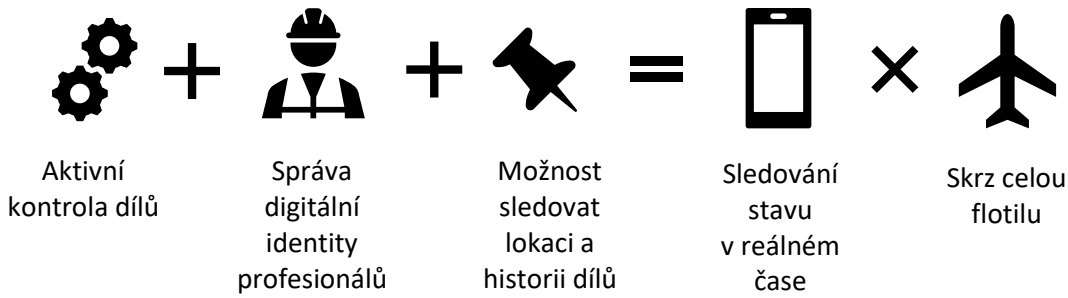
Zavedení blockchainových sítí do letecké dopravy může mít ohromné ekonomické dopady. Získání přesnějšího přehledu o historii údržby a konfiguraci letounu, může pomoci drasticky snížit náklady za jejich neplánovanou údržbu. Snížení cen za údržbu a opravu letounů se za pomoci Blockchainu očekává až 5%, což je napříč průmyslem přibližně 3,5 miliardy amerických dolarů. Celkově bude možné zvýšit životnost letounů. Ve světě je dnes provozováno přes

25 000 letounů, ze kterých přibližně polovina je zakoupena na leasing. Leasingové služby tak poskytují velice významný faktor zajišťující flexibilitu a následný růst průmyslu. Na konci leasingových období je však nutné letouny velmi důkladně zrevidovat a vyhodnotit jejich hodnotu. Tento proces je časově a finančně náročný. Nehledě na omezenou možnost kontroly důvěryhodnosti dat. Díky blockchainu mohou mít letouny na konci leasingových období mnohem vyšší hodnotu, zároveň bude historie jejich provozu a údržby transparentní. Transparentnost zajistí zvýšení důvěry mezi kupujícím a prodávajícím a zároveň sezvýší celková bezpečnost provozu, která může nejen zvýšit výnosy a zároveň ochránit lidské životy. Trh se secondhandovými letouny by tak získal na důvěryhodnosti. Zabránilo by se také podvodným praktikám při prodeji letadel a náhradních dílů. V některých případech se letecké společnosti, nebo poskytovatelé MRO služeb neobejdou bez součástek, které výrobci letounů samostatně neposkytují, nebo z obchodních důvodů je samostatně neprodávají. V takových případech se obracejí na sprostředkovatele specializované na přeprodej náhradních dílů. Sprostředkovatelé v mnoha případech spekulují s díly, kterými v daný moment nedisponují. Tím vzniká prostor pro nečestné jednání. Přidávají k ceně dodatečné poplatky a často nemohou zajistit jejich včasné doručení. Blockchain by zde byl ideálním řešením. Každá součástka by měla svůj oficiální otisk v globální databázi. Podle sériového čísla by bylo možné zjistit jaká je historie součástky a kdo ji v danou chvíli vlastní. Sprostředkovatelé, by tak nemohli kupujícím v průběhu obchodu přidávat dodatečné poplatky a dodávat nekompletní informace o historii dílů. Zajištěním důvěryhodných dat je možné zároveň změnit pohled na pojištění letadel. Pojištění se u většiny leteckých společností vytváří pro celou letku. Hodnota letounů však v průběhu jejich provozu osciluje a částka, na kterou jsou pojištěny mnohdy neodpovídá. Zvýšením transparentnosti stavu každého z letadel, by tak bylo možné zajistit efektivnější výpočet cen za pojistného, které by dynamicky reagovalo na stav letounů. Z tohoto faktu by těžili nejen provozovatelé letounů, ale i entity nabízející pojištění. Analýza společnosti PwC předpovídá, že efektivita získaná využíváním blockchainových sítí by zvýšila hodnotu celého trhu s letadly o 4%, což je přibližně 40 miliard amerických dolarů. [25]

12.2 Praktické výhody

Blockchain by mohl pomoci změnit filozofii údržby. Z reaktivní principu, na přístup proaktivní. Reaktivní přístup znamená řešení problému až ve chvíli kdy se projeví. Díly jsou tak velice často již nefunkční, nebo náklady na jejich opravu jsou pro aerolinku finančně a časově náročné. Proto se v údržbě letadlové techniky vytvořila filozofie proaktivní. Letadlo je podrobováno častým kontrolám, kde je průběžně sledován stav životně důležitých dílů. Díky

tomu se zabrání zbytečným nákladům na nečekané opravy a z toho vzniklých dodatečných provozních nákladů. Sledování průběžné životnosti součástek by pomocí blockchainových databází umožnilo vytvoření oficiální digitální dokumentace, ke které by měli přístup nejen mechanici, ale i autority, které letuschopnost letadel kontrolují. Digitální klíče a podpisy by tak mohly zcela nahradit papírovou verzi a pomohly v rychlejší, ekonomičtější a transparentnější komunikaci mezi účastníky kontroly letové způsobilosti. Další výhodou by byl efektivní způsob sběru velkých dat. Velká data v kombinaci s umělou inteligencí by pomáhala vytvořit databáze pro řešení závad. Díky efektivnímu sběru dat by bylo možné řešit slabé stránky konstrukce systémů letadel a dále tak rozvinout bezpečnost provozu letounů. Výrobci letadel by pomocí těchto dat mohli efektivněji reagovat na technické výzvy, které by mohli aplikovat do nových konstrukčních řešení. Aktivní sledování součástek by mohlo pomoci nahradit záruky, za garance. Záruky pomáhají provozovatelům letadel držet ceny za údržbu na udržitelné hodnotě, ale za cenu nedostatečného reaktivního času. V budoucnosti by výrobci za pomoci Blockchainových sítí mohli garantovat životnost součástek. Za pomoci čidel, které by fungovali jako IoT, by bylo možné nastavit systémy na automatická upozornění na potřebu údržby, či výměny dílu a s tím spojené objednávání součástek. Efektivní způsob dodávání náhradních součástek, by tak mohl provozovatelům letadel snížit náklady na skladování dílů. Zároveň by tak snížil pracovní zátěž personálu a dovolil jim věnovat se závažnějším problematice. Aby letecká technika byla letuschopná pro komerční provoz, je nutné v součtu vynaložit obrovský počet člověko-hodin. Kvalifikovaný personál se stává čím dál tím víc nákladným artiklem. Letečtí mechanici, stejně jako letecké posádky, mají různé kvalifikace a pravomoci v provádění úkonů údržby. Skutečně efektivní způsob managementu těchto profesionálů je velice organizačně náročný. Propojením blockchainové sítě pro údržbu letounů a sítě pro managementu leteckým mechaniků by se tak dalo docílit velmi efektivního ekosystému, ze kterého by těžili všechny strany od výrobců letadel až po cestující.



Obrázek 29 Přínos blockchainu do údržby letadel [25]

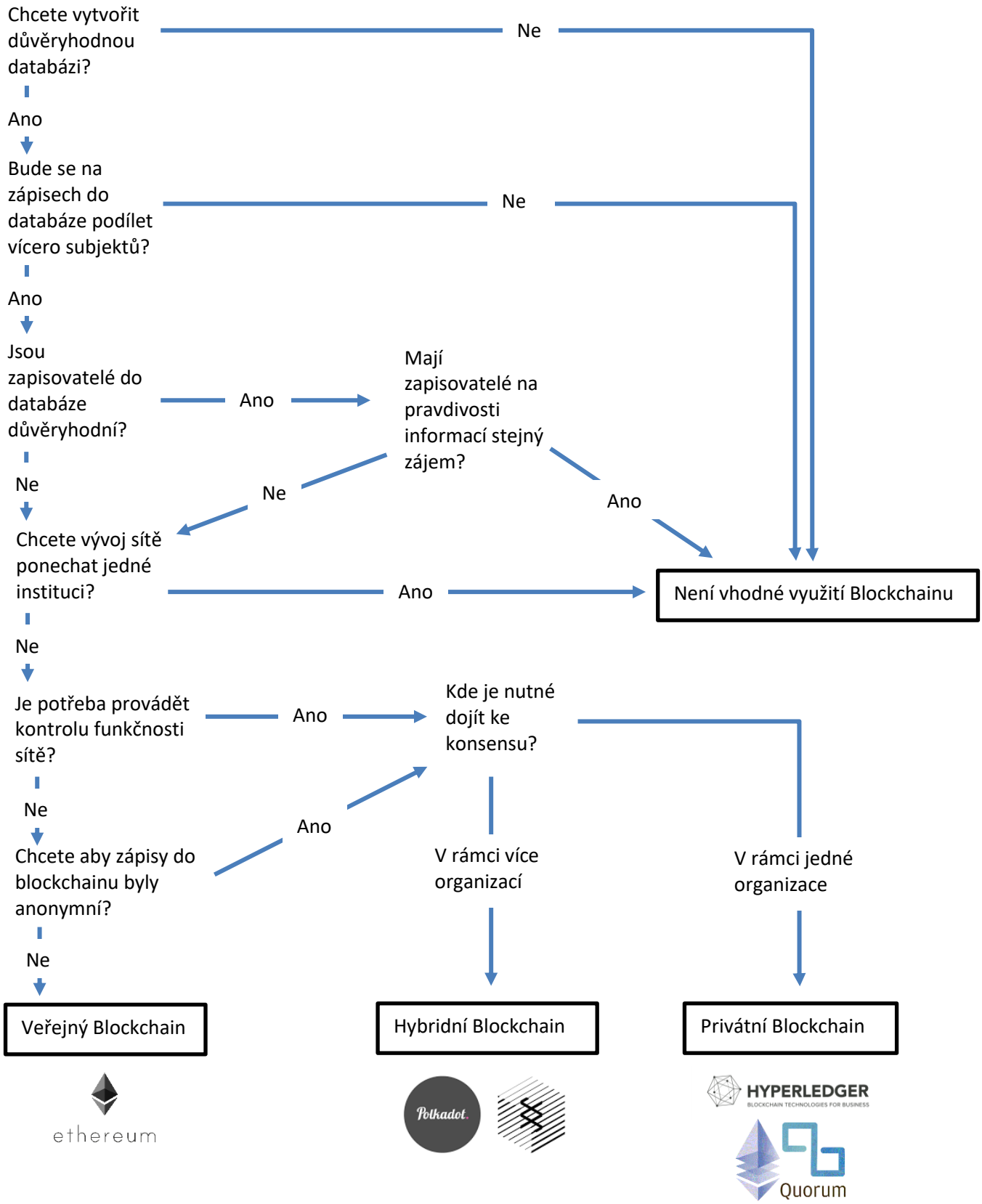
13 Tvorba projektů

Tvorba projektů je jedna ze zásadních problematik využitelnosti blockchainu. Základní otázkou tak musí být, zda je blockchain pro dané využití vůbec vhodný. Blockchain je ideální pro využití v prostředí kde nutná rychlá spolupráce více stran, které si musí vyměňovat důvěryhodná data, obsahující potvrzení časového otisku a podpisu tvůrce. Dále je využitelný v prostředích, kde je nutné se zbavit prostředníků a zprostředkovatelů služeb, kteří přidávají do sítě potenciál netransparentnosti a složitosti. Letectví bezpochyby takovým prostředím je. Velký počet projektů zakládajících se na technologii blockchain končí v počáteční fázi. Tvůrci velice často zjistí, že investovaný čas a zdroje nebudou vést k tíženému zlepšení. Důvodem je snaha o tvorbu přespříliš komplexní sítě, na kterou legislativa, průmysl a lidé zatím nejsou připraveni. Aby bylo možné spustit reálnou blockchainovou síť, je nutné vytvořit rozsáhlý ekosystém, který bude poskytovat výhody pro všechny zúčastněné. Jakmile se podaří vybudovat důvěru a přesvědčit většinu potencionálních účastníků o výhodách elektronické identity, nebo tvorby globální databáze pro údržbu letadel, stane se z decentralizovaných databází nenahraditelný nástroj, stejně jako se jím staly počítače a internet. Ideálním prostředím pro vznik projektů jsou ekosystémy univerzit. Univerzity jsou více, či méně celosvětově propojené instituce, které mají lacinou a počítačově vzdělanou pracovní sílu. Při správné motivaci je pomoci grantů možné vytvořit malé projekty, které by se soustředily na vývoj uzavřených blockchainových sítí, s jednoduchým využitím. Následně by bylo možné oddělené projekty začít spojovat a vytvářet větší a tím pádem v reálném světě použitelnější síť. Zásadní pro vývoj blockchainu je, aby na něm získaly výhody všichni zúčastněný. Toho je možné dosáhnout jedině, pokud projekt není tvořen pouze jedním subjektem, ale širokou škálou společností a uživatelů, které se na ekosystému sítě podílejí.

13.1 Základní určení sítě

Tvůrci sítí po důkladném uvážení využitelnosti blockchainu pro daný projekt musí zjistit, jakou z architektur mohou pro svůj projekt využít. K dispozici jsou privátní, veřejné a hybridní blockchainy, nabízející rozdílné uchopení problematiky. Každý přístup má své výhody a nevýhody, které je nutné důkladně zvážit. Veřejné sítě nabízejí obrovský potenciál demokratického rozhodování, ale pro průmyslové využití jsou zatím příliš neuchopitelné. Základním problémem je nemožnost vytvářet škálovatelný přístup. Zároveň naprostá anonymita uživatel nepodporuje důvěryhodnost sítě mezi samotnými uzly sítě a zároveň mezi uzly sítě a státními orgány. Privátní a hybridní sítě nabízí pro letectví mnohem užitečnější

nástroj. Díky blockchainovým sítím bude možné vytvářet velmi efektivní dodavatelské řetězce, sítě pro správu rezervací letenek a privátních letounů, nebo správu věrnostních programů aerolinek. Blockchainové sítě zefektivní přístup k ochraně osobních dat zákazníků a dají aerolinkám silný nástroj pro poznávání chování zákazníků, takzvané KYC (Know Your Custommer). Tento potenciál již spatřilo v Blockchainu několik velkých softwarových a hardwarových gigantů, jako jsou IBM Intel, Microsoft, nebo Google. Tyto firmy se snaží vytvářet komunity a nástroje, které mají napomáhat rozvoji decentralizovaných privátních sítí. Spolu s nimi jsou tvořeny konsorcia typu Hyperledger, která působí jako inkubátory aplikací pro vytváření blockchainových sítí. Konsorcia se snaží vytvářet open – source zdroje informací, propojují nápady a hlavně profesionály napříč obory, kteří vidí v Blockchainu potenciál. Nejlepší možností se jeví hybridní sítě, které mají slučovat dobré vlastnosti privátních i veřejných sítí, při zachování decentralizace a bezpečnosti. Diagram níže má za úkol pomoci tvůrcům projektů s rozhodováním, které řešení sítě je pro ně nejvýhodnější.



Obrázek 30 Pomůcka pro určení platformy [Autor]

Aplikací tohoto pravidla je možno analyzovat příklady využití v této práci. U využití Blockchainu pro tvorbu elektronické identity je potřeba využít důvěryhodnou databázi. Blockchain pro kontrolu letové způsobilosti je také nutné vytvořit jako důvěryhodnou databázi, kde bude moci informace do blockchainu zapisovat více různých organizací s různou úrovní důvěryhodnosti. Vývoj sítě však není možné ponechat jedné organizaci, protože je zde mnoho organizací, které mají rozdílné zájmy a tím pádem je nutné aby se na vývoji podílely stejnou měrou. Zároveň aby byla funkčnost sítě zajištěná je nutné, aby ke konsensu docházelo mezi více organizacemi s různým polem působnosti, tím pádem i pro tuto aplikaci je nejvhodnější využít Hybridního přístupu.

V případě využití blockchainu pro digitalizaci dat o letadlové technice, je nutné vytvořit důvěryhodnou databázi. Do databáze bude zapisovat mnoho účastníků sítě, s různou úrovní důvěryhodnosti. Aby mohlo vzniknout prostředí s rovnými podmínkami, je nutné aby se na tvorbě takové sítě podílelo co nejvíce subjektů. Kvůli nutnosti vysoké důvěryhodnosti dat, bude dále potřeba, aby byla síť průběžně kontrolována a upravována. Tím, že se jedná o velmi mnoho subjektů, které se na síti podílejí, je nutné vytvořit Hybridní síť.

13.2 Financování projektů

Způsoby financování projektů se vyvíjejí od počátku historie blockchainu. Nejvíce používaná metoda do roku 2018 bylo Initial Coin Offrenig (ICO). Jedná se o typ crowdfundingu, kdy je představen projekt veřejnosti. Veřejnost pak pomocí kupování tokenů projekt podpoří. Finance nasbírané tímto způsobem jsou následně tvůrci sítě použity na její vývoj a provoz. Zakoupené tokeny mohou uživatelé v rámci sítě využívat, nebo je zpět proměnit ve směnárnách za reálné peníze. Problematické se ICO ukázalo v roce 2018 z důvodu nedostatečné kontroly nad vývojem. Mnoho ICO tak vybralo v crowdfundingu finance na projekty, které se kvůli špatnému business plánu nikdy nezrealizovaly. Některé studie ukazují, že až 80% ICO v roce 2018 bylo vytvořeno s nerealistickými plány, nebo s úmyslem získat finance a nikdy nedoručit finální produkt. Dalším vývojovým stupněm se stalo Security Token Offering, zkráceně STO. STO nabídlo možnost investovat do rozvoje sítě pomocí Security tokenů. Security token je v analogii reálného světa něco jako akcie. Je podložená reálným vlastnictvím části sítě a z ní vycházejících profitů. Problém s STO je vysoká regulace v rámci USA a Evropské unie, kde projekty bojují s velkým množstvím byrokratických úkonů. Tím se stává pro tvůrce sítě příliš finančně a časově náročné. Kvůli přílišné robustnosti se v roce 2019 objevil nový způsob financování Initial Exchange Offering, zkráceně IEO. IEO spočívá na stejném principu jako ICO. Jde o crowdfunding založený na prodeji tokenů. Na rozdíl od ICO jsou tyto startupy

zaštítěny směnárnami kryptoměn. Prostředí směnáren zajistí tvůrcům marketingový prostor, kde mohou své projekty zveřejňovat. Směnárny následně získávají procenta z prodaných tokenů. Společně s tokeny získávají i výhody ze zapojení jejich služeb do nových projektu. Směnárny tím pádem mají přímý zájem realizovatelnosti projektů. V poslední době se však trh vrací ke klasickému typu investování nazývanému Venture Capital. Projekty hledají investory z reálného businessu, kteří mají v rozvoji decentralizovaných sítích zájem. V leteckém průmyslu se může jednat o podporu ze strany výrobců letadel, leteckých společností, nebo organizací zaštiťující civilní letectví. U studentských projektů se tak může jednat o granty od univerzit, či konsorcií zabývajících se rozvojem blockchainových sítí. [26]

14 Závěr

V diplomové práci jsem rozvinul myšlenku implementace blockchainových sítí do civilního letectví. Jde o novou technologii, která bude v leteckém průmyslu nacházet čím dál více využití. Stabilita leteckého průmyslu závisí na mnohých faktorech, které mohou a nemusí být zaviněny lidským faktorem, jak můžeme pozorovat například při současné krizi s pandemií COVID-19. Pro snížení dopadů budoucích krizí je proto žádoucí, aby šlo letectví aplikacích inovací příkladem, ostatním odvětvím průmyslu. Osvojením si nejnovějších trendů ve vývoji bude možné nadcházející hrozby rychleji rozeznávat a překonávat. Efektivnější identifikace osob může zvýšit propustnost letišť a tím snížit kontakt cestujících mezi sebou, nebo kontakt cestujících s leteckým personálem. Nemoc COVID-19 však, jen umocnil již déle trvající krizi způsobenou uzemněním nové verze nejvyužívanějšího letounu na světě, Boeing 737 MAX. Nedostatečná transparentnost ve vývoji, údržbě a nedostatečný sběr informací o provozu letounu znamenalo ztrátu několika set životů a nevyčíslitelné ztráty pro letecký průmysl, který se z těchto ran může vzpamatovávat ještě několik dalších let. Blockchain může pomoci i v případě výroby, údržby a prodeje letounů. Nastartuje průmysl do nové digitální doby, kde informace budou veřejně dostupné, přehledné a nezmanipulovatelné. Jako každá nová technologie, i blockchain skýtá mnoho výzev, ale prozatím i nedořešené problematiky. Jeho potenciál je však pro letectví bezpochyby obrovský. Trend, který potvrzuje rozmach sociálních sítí ukazuje, že uživatelé již v plné míře nedůvěřují státním a centralizovaným zdrojům informací. Blockchain by takto dal vzniknout sítím působícím nadnárodně. Účastníci sítě by se sami podíleli na vývoji, kterým se celý trh bude vydávat. Oficiální autority by následně byly nuceny tyto trendy akceptovat a přizpůsobit se jim. Z ekosystému blockchainu mohou dlouhodobě těžit všechny zainteresované strany. Bohužel je vývoj těchto sítí velmi náročný na lidské i finanční zdroje, proto nutné začít do projektů investovat co nejdříve, aby bylo možné začít využívat potenciálu blockchainu v dohledné době. Obrovské investice ze strany softwarových i hardwarových společností nám dávají naději, že technologie i přes svoji momentálně nedostatečnou rozvinutost, bude moci svůj potenciál naplnit poměrně brzo a pomůže následnému rozvoji napříč průmysly.

Cíl práce považuji za splněný. Práce může v případě zájmu o realizaci projektů sloužit jako zdroj základních informací pro využití v letectví a všeobecná inspirace. Řeší základní problematiku, jakým směrem se ve vývoji posouvat a jak projekty financovat. V práci jsem přiblížil nejnovější trendy ve vývoji decentralizovaných databází a zároveň je aplikoval pro možné využití v oblasti leteckého průmyslu. Na jejím základě je možné v univerzitním prostředí

vytvořit malé projekty zabývající se vývojem zejména privátních, které budou zvyšovat povědomí společnosti a touhu řešit zatím nekonfrontované problémy. Takový trend by mohl později přinést propojování menších projektů a vytváření spolupráce mezi fakultami, univerzitami a budoucími zaměstnavateli. Takové prostředí dá vzniknout novým příležitostem jak pro studenty, absolventy, tak pro vyučující, kteří se budou moci zapojit do tvorby velmi aktuálních projektů a start-upů. Takto připravení profesionálové budou mít náskok oproti svým kolegům a budou moci nově nabyté zkušenosti uplatnit napříč obory, v zajímavých a lukrativních příležitostech.

15 Seznam literatury a informačních zdrojů

[1] FUTURE OF THE AIRLINE INDUSTRY 2035. IATA Official website [online]. Montreál: IATA, 2019 [cit. 2020-04-01]. Dostupné z: https://www.iata.org/contentassets/690df4ddf39b47b5a075bb5dff30e1d8/iata-future-airline-industry-pdf.pdf

[2] JOSEPHS, Leslie. Wall Street expects Boeing to take another big, ugly charge on 737 Max. BofA estimates total cost of crisis as high as $20 billion. *CNBC* [online]. CNBC LLC., 2020, 17.1.2020 [cit. 2020-04-01]. Dostupné z: https://www.cnbc.com/2020/01/17/737-max-crisis-could-cost-boeing-as-much-as-20-billion-wall-street.html

[3] Air transport, passengers carried. *The World Bank* [online]. Chicago: The World Bank group, 2019 [cit. 2020-04-01]. Dostupné z: https://data.worldbank.org/indicator/IS.AIR.DPRT

[4] Commercial Market Outlook 2019 – 2038. Boeing the Company [online]. Chicago: Boeing the Company, 2019 [cit. 2020-04-01]. Dostupné z: http://www.boeing.com/commercial/market/commercial-market-outlook/

[5] LASTOVETSKA, Anastasiia. Basics: Components, Structure, Benefits & Creation. MLSDev [online]. MLSDev, 2019, 31. 1. 2019 [cit. 2020-03-19]. Dostupné z: https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture

[6] What Is a Block in the Blockchain? Medium [online]. Medium, 29. 12. 2018 [cit. 2020-03-19]. Dostupné z: https://medium.com/datadriveninvestor/what-is-a-block-in-the-blockchain-c7a420270373

[7] What's the Maximum Ethereum Block Size? ETH Gass station Blog [online]. ETH Gass station, 2019, 25. 9. 2019 [cit. 2020-03-19]. Dostupné z: https://ethgasstation.info/blog/ethereum-block-size/

[8] SHA256 [online]. 2017 [cit. 2020-03-19]. Dostupné z: https://emn178.github.io/online-tools/sha256.html

[9] International Air Transport Association (IATA) [online]. Montreál: International Air Transport Association (IATA), 2020 [cit. 2020-03-19]. Dostupné z: https://www.iata.org/en/services/finance/airlines

[10] MILLER, Seth. IATA Coin: A blockchain play by and for the airline world. PAXEX.AERO [online]. Proton Associates, 2020, 14 DECEMBER 2018 [cit. 2020-03-19]. Dostupné z: https://paxex.aero/2018/12/iata-coin-a-blockchain-play-by-and-for-the-airline-world/

[11] Byzantine Fault Tolerance Explained. Binance Academy [online]. Binance.com, 2017, 2018 [cit. 2020-03-19]. Dostupné z: https://www.binance.vision/blockchain/byzantine-fault-tolerance-explained

[12] CONSENSUS MECHANISMS. Horizen ACADEMY [online]. Horizen: Horizen, 2019 [cit. 2020-03-19]. Dostupné z: https://academy.horizen.global/technology/advanced/consensus-mechanisms/

[13] CURRAN, BRIAN. What is Proof of Elapsed Time Consensus? (PoET) Complete Beginner's Guide. Blockonomi [online]. Blockonomi: KOOC MEDIA, 2018 [cit. 2020-03-19]. Dostupné z: https://blockonomi.com/proof-of-elapsed-time-consensus/

[14] PEH, Bernard. What are Public, Private and Hybrid Blockchains? *Medium* [online]. Medium, 2018, 10.11. 2018 [cit. 2020-05-04]. Dostupné z: https://medium.com/@blockchain101/what-are-public-private-and-hybrid-blockchains-e01d6e21eb41

[15] SKVORC, Bruno. Introduction to Ethereum: A Cryptocurrency with a Difference. *Sitepoint* [online]. Sitepoint, 2018, 15.5. 2018 [cit. 2020-05-04]. Dostupné z: https://www.sitepoint.com/ethereum-introduction/

[16] TAKYAR, Akash. TOP BLOCKCHAIN PLATFORMS OF 2020. *Sitepoint* [online]. Leewayhertz, 2020, 2020 [cit. 2020-05-04]. Dostupné z: https://www.leewayhertz.com/blockchain-platforms-for-top-blockchain-companies/

[17] TAKYAR, Akash. Jack Platts. *Medium* [online]. Medium, 2019, 14.2. 2019 [cit. 2020-05-04]. Dostupné z: https://medium.com/polkadot-network/polkadot-the-foundation-of-a-new-internet-e8800ec81c7

[18] ATTACKS ON BLOCKCHAIN. Horizen ACADEMY [online]. Horizen: Horizen, 2019 [cit. 2020-03-19]. Dostupné z: https://academy.horizen.global/technology/advanced/attacks-on-blockchain/

[19] What are Oracles? Smart Contracts, & "The Oracle Problem". Medium.com [online]. Medium, 2019 [cit. 2020-03-19]. Dostupné z: https://medium.com/@teexofficial/what-are-oracles-smart-contracts-the-oracle-problem-911f16821b53

[20] Jura Protocol Media. Blockchain Oracles Explained. Medium [online]. Medium, 2019 [cit. 2020-04-01]. Dostupné z: https://medium.com/@juraprotocol/asymmetric-encryption-blockchain-cryptography-e78348fbff78

[21] Symmetric vs. Asymmetric Encryption. *Binance Academy* [online]. Binance.com, 2017 [cit. 2020-04-01]. Dostupné z: https://www.binance.vision/security/symmetric-vs-asymmetric-encryption

[22] TYPES OF WALLETS. Horizen ACADEMY [online]. Horizen: Horizen, 2019 [cit. 2020-03-19]. Dostupné z: https://academy.horizen.global/technology/advanced/types-of-wallets/

[23] LUNDEN, Ingrid. UK's ICO fines British Airways a record £183M over GDPR breach that leaked data from 500,000 users. Tech Crunch [online]. Verizon Media, 2019 [cit. 2020-03-19]. Dostupné z: https://techcrunch.com/2019/07/08/uks-ico-fines-british-airways-a-record-183m-over-gdpr-breach-that-leaked-data-from-500000-users/

[24] Sovrin™: A Protocol and Token for SelfSovereign Identity and Decentralized Trust. A White Paper from the Sovrin Foundation [online]. 2018, 2018(1), 42 [cit. 2020-03-23]. Dostupné z: https://sovrin.org/wp-content/uploads/2018/03/Sovrin-Protocol-and-Token-White-Paper.pdf

[25] Data for the life of the aircraft. *PwC* [online]. PwC, 2019, Duben 2019 [cit. 2020-04-01]. Dostupné z: https://www.pwc.com/gx/en/aerospace-defence/assets/data-for-the-life-of-the-aircraft.pdf

[26] SINHA, Sritanshu. IEOs, ICOs, STOs and Now IDOs — How to Raise Funds for Crypto in 2019? *Cointelegraph* [online]. Cointelegraph, 2019, 1.9. 2019 [cit. 2020-05-04]. Dostupné z: https://cointelegraph.com/news/ieos-icos-stos-and-now-idos-how-to-raise-funds-for-crypto-in-2019

16 Seznam obrázků