Využití technologie blockchain pro decentralizované ověřování identity

Bc. Vítězslav Zich

Diplomová práce
2023

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav informatiky a umělé inteligence

Akademický rok: 2022/2023

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Vítězslav Zich**
Osobní číslo:	**A20698**
Studijní program:	**N0613A140022 Informační technologie**
Specializace:	**Kybernetická bezpečnost**
Forma studia:	**Kombinovaná**
Téma práce:	**Využití technologie blockchain pro decentralizované ověřování identity**
Téma práce anglicky:	**Use of Blockchain Technology for Decentralized Identity Verification**

Zásady pro vypracování

1. Proveďte literární rešerši a popište technologii blockchain.
2. Pozornost věnujte také problematice SSI (Self Sovereign Identity).
3. Teoreticky nastudujte a popište proces vystavení elektronického dokladu identity
4. Zmapujte iniciativu Evropské unie pro blockchainovou infrastrukturu EBSI (European Blockchain Services Infrastructure) a dále ESSIF (European Self Sovereign Identity Framework).
5. Navrhněte a implementujte vystavení elektronického dokladu (verifiable credential) identity a jeho ověření.
6. Diskutujte i aplikaci evropských standardů a doporučení EU do SSI.

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. PREUKSCHAT, Alex and Drummond REED. Self-Sovereign Identity: Decentralized digital identity and verifiable credentials: Decentralized digital identity and verifiable credentials. New York, NY: Manning Publications, 2021. ISBN 9781617296598.
2. BASHIR, Imran. Mastering Blockchain: A deep dive into distributed ledgers, consensus protocols, smart contracts, DApps, cryptocurrencies, Ethereum, and more, 3rd Edition. 3. ed. Birmingham, England: Packt Publishing, 2020. ISBN 9781839213199.
3. LIPTON, Alexander and Adrien TRECCANI. Blockchain and distributed ledgers: Mathematics, technology, and economics. Singapore, Singapore: World Scientific Publishing, 2021. ISBN 9789811221521.
4. BALDACCI, Emanuele and Joao Rodrigues FRADE. Advancing digital transformation in the public sector with blockchain: A view from the European union. In: Disintermediation Economics. Cham: Springer International Publishing, 2021, pp. 281–295. ISBN 9783030657802.
5. PRIETO, Javier et al., eds. Blockchain and Applications: 3Rd International Congress. 1. ed. Cham, Switzerland: Springer Nature, 2021. ISBN 9783030861612.
6. *NGI eSSIF-Lab* [online]. Next Generation Internet Initiative, 2022 [cit. 2022-11-30]. Dostupné z: https://essif-lab.eu

Vedoucí diplomové práce: **Ing. Radek Vala, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **2. prosince 2022**
Termín odevzdání diplomové práce: **26. května 2023**

doc. Ing. Jiří Vojtěšek, Ph.D.
děkan

prof. Mgr. Roman Jašek, Ph.D., DBA
ředitel ústavu

Ve Zlíně dne 7. prosince 2022

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 26. 5. 2023 Vítězslav Zich, v. r.

ABSTRAKT

Diplomová práce se zabývá problematikou decentralizované identity s využitím blockchainu. V teoretické části jsou popsány všechny technologie a frameworky nutné pro pochopení celého ekosystému decentralizované identity a blockchainu s důrazem na aktuální stav implementace takového systému v Evropské unii. V praktické části je implementován návrh identity systému, který svým řešením nabízí nejen možnost nahradit používání hesel pro autentifikaci, ale především umožní úplnou kontrolu nad svou identitou. Diskutována je také aplikace daného systému do evropské blockchainové infrastruktury.

Klíčová slova: blockchain, decentralizovaná identita, EBSI, SSI, verifiable credentials

ABSTRACT

The diploma thesis focuses on the topic of decentralized identity in par with blockchain usage. Theoretical part describes all necessary technologies and frameworks needed for an understanding of decentralized identity ecosystem and blockchain with an emphasis of the application in European union. In practical part decentralized identity system is implemented which offers not only the possibility of replacing standard password for the authentication but above all it offers complete control over your identity. The applicability of the system into european blockchain infrastructure is discussed.

Keywords: blockchain, decentralized identity, EBSI, SSI, verifiable credentials

Chtěl bych tímto poděkovat vedoucímu mé DP, panu Ing. Radku Valovi, Ph.D. za jeho ochotu, rady a připomínky při vypracování diplomové práce. Dále bych chtěl poděkovat mé rodině a blízkým za podporu během studia.

Prohlašuji, že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

ÚVOD

V nynější době takřka každý jednotlivec na světě využívající digitální služby produkuje svoji digitální stopu. Tato stopa či záznamy jsou nedílnou součástí téměř každého z nás i přestože se můžeme tomuto trendu bránit. Například pasivitou v oblasti sociálních sítí, blokováním cookies či senzorů pohybu. Jakákoliv činnost totiž v internetu produkuje data o uživateli, jeho chování a interakci v jednotlivých systémech, kde jsou tyto údaje analyzovány. Především u velkých technologických společností dochází k profilování u uživatelů. V rámci Evropské unie již máme z pohledu jednotlivce právní základy pro omezení zpracování našich dat. Tím pádem tyto rámce poskytují i možnou kontrolu nad jejich zpracováním, čímž tyto technologické společnosti limitují. Nicméně nám neposkytují přímou kontrolu jednotlivce nad daty, které chceme sdílet.

Prvním krokem k získání kontroly nad vlastními daty může být koncept decentralizované identity, která ve své podstatě převádí správu své vlastní identity zpět na jednotlivce. Jednotlivec si poté bude moci zvolit, jaké údaje o své osobě bude chtít sdílet, a především s kým. Decentralizovaná identita totiž není jen o identitě, ale i o vztazích mezi jednotlivci či organizacemi. V diplomové práci se budeme zabývat, tzv. „Self Sovereingn Identity“ (SSI), což si v doslovném překladu můžeme přeložit jako „sebe svrchovaná identita“. SSI využívá prvky decentralizace pro dosažení svého cíle, a to prostřednictvím blockchainových technologií.

V teoretické části diplomové práce jsou uvedeny nejdůležitější vlastnosti a využívané technologie blockchainových řešení, které jsou nutné k získání základní znalosti o možnostech využití blockchainu. Následně jsou diskutovány blockchainové frameworky. Teoretická část také obsahuje znalostní rámec identity, a to především nových konceptů SSI, které se vzhledem ke svému masivním vývoji v poslední době velmi posouvají dopředu. Na poli digitální identity probíhá v Evropské unii intenzivní vývoj evropské blockchainové infrastruktury, který je v rámci práce diskutován z pohledu legislativy, tak i reálných požadavků a implementací.

V praktické části práce je vytvořen návrh řešení decentralizované identity z pohledu celého ekosystému SSI. Je proveden návrh infrastruktury všech zúčastněných stran SSI. Pro ukázkové řešení jsou definovány stěžejní role a operace pro vydávání a ověřování identity. Následně jsou popsány jednotlivé komponenty SSI ekosystému, které jsou v řešení implementovány a diskutovány z pohledu dalších možnosti vývoje komponent. Na závěr praktické

části je prezentováno ukázkové řešení z pohledu uživatele a jeho interakcí s vydavatelem a ověřovatelem identity.

Na závěr práce je evaluována implementace s diskuzí potencionálního rozšíření z pohledu připojení do evropského ekosystému.

I. TEORETICKÁ ČÁST

1 BLOCKCHAIN

Blockchain je v posledních letech skloňován jako revoluční koncept využívající kombinaci technologií, který vytváří ideální podmínky pro rozšíření myšlenky decentralizace systémů. V následujících kapitolách jsou uvedeny jednotlivé technologie a principy, které tento koncept dostaly do reálné podoby.

1.1 Definice

Blockchainová technologie je ze své podstaty velmi komplexní, nicméně existují dvě všeobecně uznávané definice:

Definice dle Laymana

„Blockchain je systém sdílející vedené záznamy, kde každý účastník uchovává identickou kopii chronologicky seřazených záznamů. Účastník může přidat nové záznamy pouze v případě, že s tím kolektivně souhlasí.“

Obecně uznávaná technická definice

Blockchain je peer to peer „distribuovaná účetní kniha“, která je zabezpečená kryptografií, je možné záznamy pouze přidávat a je neměnná (je ji velmi obtížné změnit) a lze ji aktualizovat pouze na základě konsenzu mezi uživateli peer to peer sítě. [1]

1.2 Historie

První koncept technologie blockchainu byl uveden v roce 2008 v publikaci “Bitcoin: A Peer-to-Peer Electronic Cash System“ od organizace či jednotlivce s pseudonymem Satoshi Nakamato. Na základě publikace byla od stejné skupiny tato technologie poprvé implementována v roce 2009 jako kryptoměna Bitcoin, kterou známe i dnes. [1]

V letech 2012 až 2013 došlo k první vlně popularizace blockchainových technologií a bitcoinu. Vzhledem k tomuto faktu vznikly nové projekty, z nichž nejznámější jsou např. Quorum, Corda a především Ethereum. Tyto blockchainové frameworky jsou provozovány až do dnešní doby.

1.3 Komponenty blockchainu

Koncept blockchainu je velmi výstižně popsán technickou definicí, viz. kapitola 2.1., uvedením základních vlastností a komponent blockchainu.

Peer to peer – V rámci blockchainu neexistuje žádný centrální bod, síť je tedy plně decentralizovaná, transakce či operace lze provádět napřímo mezi jednotlivými peery v síti.

Distribuovaná účetní kniha (tzv. digital ledger, dále DLT) – Jedná se o distribuovanou účetní knihu (databázi), která obsahuje všechny změny, každý peer v síti obsahuje kopii této DLT.

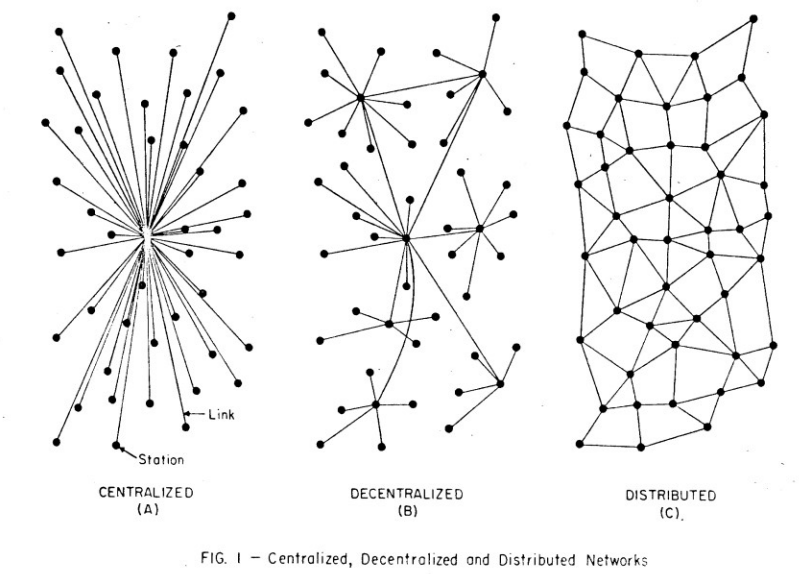
Kryptografické zabezpečení – Kryptografie je využitá pro zabezpečení DLT proti neoprávněné manipulaci a zneužití. Z pohledu kryptografie se jedná především o využití hashovacích funkcí a asymetrické kryptografie.

Záznamy lze pouze přidat (tzv. „append only“ přístup) **–** V rámci blockchainu je možné záznamy pouze přidávat, jakmile jsou data obsažená v bloku dat přidána do DLT, jsou tato data neměnná.

Aktualizovatelný prostřednictvím konsenzu – Konsenzus je nejdůležitější komponentou blockchainu, kdy nové změny v DLT jsou prováděny na základě konsenzu. Jednotlivé blockchainy používají specifické konsenzuální algoritmy, na základě kterých se validuje, zda je možné nový záznam na DLT zapsat. [2]

1.3.1 Topologie sítí

Koncept decentralizovaných a distribuovaných systémů byl představen [3] již v roce 1964 P. Baranem při návrhu sítě ARPANETU a odolnosti sítě vůči výpadkům centrálního uzlu v síti. Dělení systémů je pro práci aplikovatelné jak pro oblast blockchainu, tak do jisté míry i pro případ konceptů systémů identit, kdy existují jednotlivé nody v síti, které jsou navzájem propojeny, ale v případě selhání jakéhokoliv uzlu v síti nedojde k žádnému výpadku služby či sítě.



Obrázek 1. Topologie sítí [3]

Centralizované systémy

Veškerá komunikace je ovládána a koordinována centrální uzlem. Pokud dojde k selhání uzlu, tak dojde k nedostupnosti celé sítě.

Decentralizované systémy

V této síti existuje více cest pro přenos dat mezi uzly. Pokud dojde k selhání jednoho uzlu, komunikace může pokračovat pomocí ostatních uzlů. Tento typ sítě je robustnější a odolnější vůči chybám, ale také náročnější na správu a koordinaci.

Distribuované systémy

V tomto typu sítě je každý uzel připojen ke každému jinému uzlu v síti, což zajišťuje maximální redundanci a odolnost vůči selhání. Pokud jeden uzel selže, zbytek sítě může pokračovat v normálním provozu. Tato síťová topologie je ovšem nejnáročnější na správu a potřebuje nejvíce propojení mezi uzly. [3]

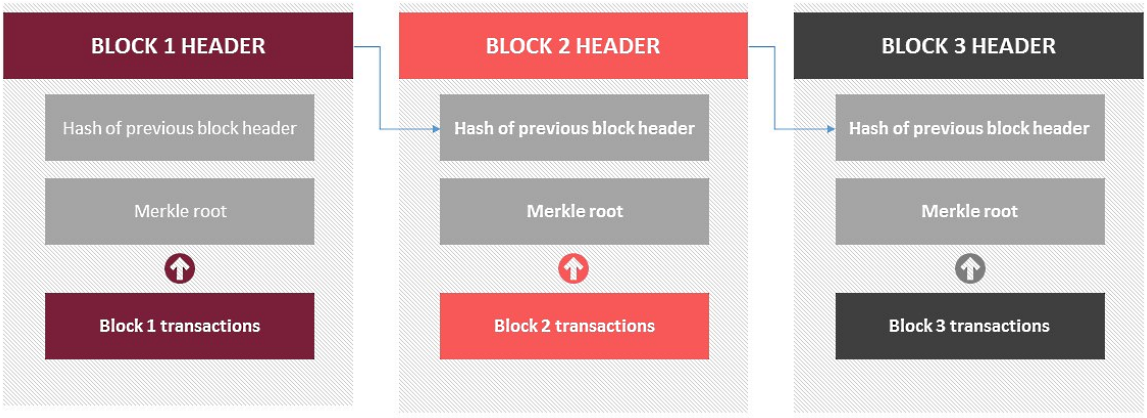
1.3.2 P2P síť

Dělení sítí lze rozdělit na základě jejich topologie, a to konkrétně na peer to peer (P2P) sítě a sítě klient-server. V architektuře klient-server, existuje jeden nebo více serverů poskytující služby klientům. V případě peer to peer sítí má každý uzel v sítí stejnou roli a data jsou

sdílena mezi jednotlivými nody. Z pohledu rezistence vůči výpadkům je P2P daleko robustnější. [4]

1.3.3 DLT

Distribuovaná účetní kniha (DLT) je decentralizovaná databáze všech transakcí, které jsou uspořádány do bloků a následně replikovány na všechny nody v rámci celé sítě. Data v rámci blockchainu jsou reprezentována jako spojený seznam (tzv. linked list) všech bloků a zároveň i ukazatelů na jednotlivé bloky. Každý blok obsahuje data a ukazatele na předchozí blok. Toto uspořádání je známo jako Merklův strom neboli hashový strom. Každý blok obsahuje hash kořene s informacemi jako je hash předchozí bloku, číslo verze bloku, seznam transakcí, časové razítko, nonci a v případě některých typů blockchainu i požadovanou časovou složitost bloku. První blok v rámci sítě je od ostatních bloků odlišný, protože neobsahuje ukazatel na přechozí blok. V blockchainové terminologii se takový blok nazývá genesis blok. Tyto popisované vlastnosti vytváří důvěru v zabezpečení dat, a především potvrzují nepopíratelnost a integritu dat. Není tedy možné pozměnit záznamy na blockchainu, jelikož by došlo ke změně hashů. Tím pádem by došlo k narušení integrity dat. [3]



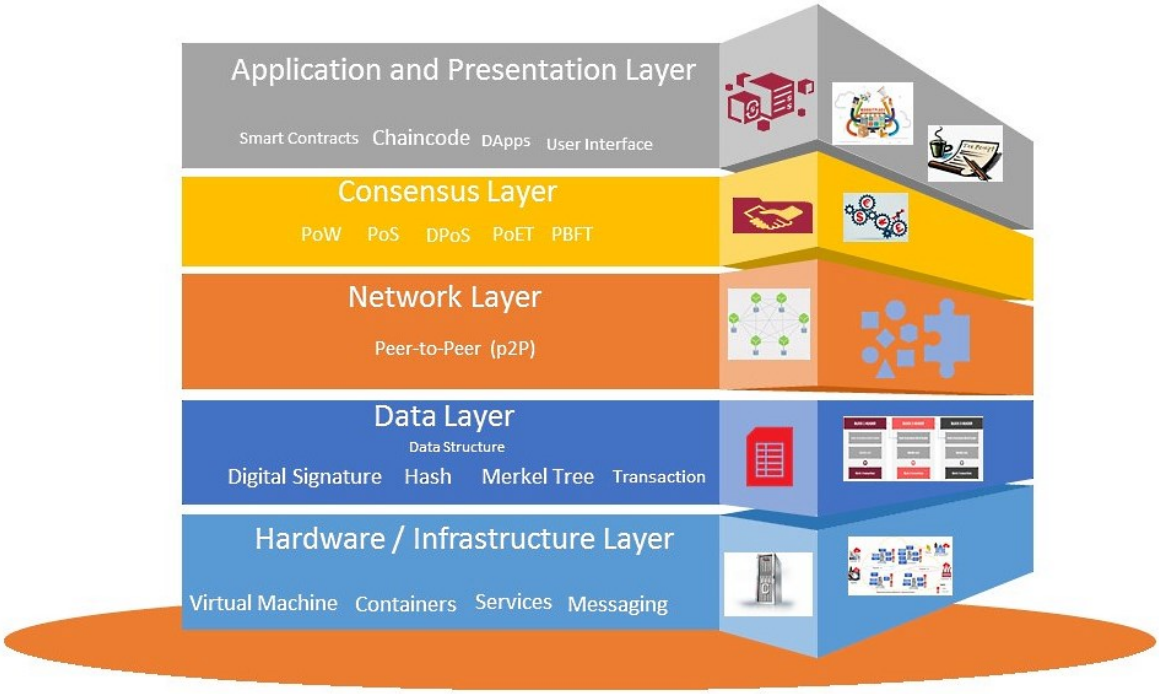
Obrázek 2. Uspořádání bloků v blockchainu [3]

1.4 Architektura blockchainu

Architekturu blockchainu členíme obecně na pět vrstev, které spolu tvoří kompletní ekosystém blockchainu.

- Hardwarová a infrastrukturní vrstva – obsahuje především, tak jako u centralizovaných aplikací, virtualizační vrstvu, operační systém, případně podpůrné systémové aplikace.

- Datová vrstva – implementuje práci s daty uloženými na blockchainu, zahrnující i kryptografii.
- Síťová vrstva – části síťové vrstvy jsou komunikační protokoly.
- Vrstva konsenzu – obsahuje implementaci konsenzuálních algoritmů.
- Aplikační vrstva – z pohledu vývojáře či uživatele se jedná o vrstvu, která s koncovým uživatelem interaguje. Jedná se o smart kontrakty, (řešeny v kapitole 1.6) či decentralizované aplikace vyvinutém nad blockchainovým frameworkem. [3]



Obrázek 3. Architektura blockchainu [3]

1.4.1 Typy blockchainu dle dostupnosti

Veřejný

Veřejné blockchainy nejsou ve vlastnictví žádné organizace. Kdokoliv se může připojit k síti a vystupovat jako uzel (nod). Pro zapojení do sítě je obecně nutné stáhnout si software, který s ostatními nody dokáže komunikovat. Dle politiky blockchainu mohou provozovatelé nodů či validátoři být odměněni za provozování nodů a validování transakcí. Právo na čtení i zápis má kdokoliv v rámci sítě po dosáhnutí konsenzu. Nejznámější veřejné blockchainy jsou Bitcoin a Ethereum.

Privátní

Privátní typ je určen pouze pro uzavřené systémy, kdy jen vydefinovaní jednotlivci či organizace v rámci konsorcia mají právo na zápis či čtení z blockchainové sítě. V rámci této organizace mají právo na zápis i čtení pouze specifické předem definované subjekty. Implementace Hyperledger Fabric blockchainu jsou typické pro tento typ blockchainu.

Semi-privátní

Jedná se o hybridní typ blockchainu, kdy řešení obsahuje jak veřejnou, tak privátní část, jež jsou od sebe odděleny. Blockchain tedy řídí jednotlivé úrovně řízení přístupu. Momentálně je tento typ spíše ve fázi návrhu a neexistuje ani žádná implementace.

V rámci dělení typu blockchainu lze rozdělit blockchain na tokenizovaný, kdy dochází ke konsenzu prostřednictvím těžení nebo prvotní distribucí nebo tzv. „tokenless“ blockchain, kdy není kryptoměna či tokeny nativní hodnotou pro nalezení konsenzu. V tomto případě se jedná především o privátní sítě, např. Hyperledger Fabric. [1]

1.5 Konsenzuální algoritmy

Konsenzus je v rámci blockchainu mechanismus, jak dosáhnout shody mezi nody v decentralizovaném systému. Tento krok je nutný ke schvalování nových bloků, a tím pádem i k synchronizaci a potvrzení nejnovějších transakcí. Každý blockchainový framework používá dle svého zaměření specifický konsenzuální algoritmus, uvedeme tedy dva nejpoužívanější ve světě kryptoměn. Existují také návrhy konsenzuálních algoritmů, které jsou pouze ve fázi návrhu, nicméně nejsou implementovány v žádném blockchainovém řešení.

1.5.1 Proof of Work

V rámci kryptoměn se jedná o jeden z nejpoužívanějších přístupů. Nový blok je schválen, a tedy vytvořen, pouze za předpokladu úspěšného vyřešení matematického problému. Tento algoritmus využívá Bitcoin a za vytvoření nového bloku dostane „težař“ odměnu v podobě tokenů. Jedná se o poměrně výpočetně náročný problém s vysokou energetickou spotřebou.

1.5.1 Proof of Stake

Jednotliví uživatelé nabízí své tokeny, tzn. svůj stake, kdy ti s největšími staky mají vyšší pravděpodobnost zvolení jako validátoři transakcí. Avšak výběr validátora je náhodný. Pokud by chtěl validátor podvádět, tak může o daný stake přijít. V případě korektní validace

transakcí dostane validátor odměnu v podobě tokenů. [1] Nejznámější implementace proof of stake konsenzu je aktuálně používána v největší blockchainové síti Ethereum. V předchozích letech Ethereum využívalo ve své síti proof of work. K přechodu dané sítě na proof of stake došlo především z důvodu daleko menších nároků na energii z pohledu provozu sítě. Každá taková větší změna v chování sítě se nazývá „hard fork“. Pokud má být hard fork platný musí na novou verzi přejít postupně všechny nody v rámci sítě.

1.6 Smart kontrakty

Smart kontrakty jsou automatizované smlouvy, jejichž pravidla jsou stanovena pomocí kódu a dat a poté dochází na jejich základě ke zprocesování. V rámci Ethereum sítě je smart kontrakt automatizovaný program, který poslouchá na své vlastní adrese. Tyto kontrakty v Ethereum síti jsou většinou psány v programovacím jazyce Solidity. Jakmile jsou tyto smlouvy nasazeny do sítě, tak jsou plně automatizované a nejsou ovladatelné jiným uživatelem. Uživatelé nicméně mohou interagovat se smart kontraktem v rámci odesílání transakcí. [1][5]

1.7 Aktuální frameworky

Na poli blockchainových frameworků v současné době převládají projekty týkající se spíše kryptoměn či NFT (Non fungible token), nicméně v posledních letech i původní kryptoměnové projekty začínají v určitém kontextu podporovat decentralizovanou identitu. V následujících podkapitolách jsou uvedeny příklady projektů, u kterých probíhá alespoň diskuze či byl prezentován tzv. „whitewaper“ v kontextu decentralizované identity.

1.7.1 Ethereum

Jedná se o kryptoměnový projekt s druhou největší tržní kapitalizací, který vznikl v roce 2013 a v roce 2015 došlo ke spuštění produkční decentralizované sítě. Ethereum přišlo s několika převratnými koncepty, a to především smart kontrakty (detailněji popsané v kapitole 1.6) a spolu s nimi i Ethereum virtual machine (EVM). EVM je výpočetní jednotka pro správu stavu Ethereum blockchainu a umožňuje zpracování smart kontraktů. EVM je tedy součástí každého klienta, který je připojen k Ethereum síti. Klientem se rozumí software provozující jeden uzel sítě. [6]

Podpora SSI v rámci Ethereum ekosystému nyní není nativní, existují nicméně tzv. EIP (Ethereum Implementation Proposal), což jsou návrhy na implementace nových funkcionalit

v rámci Ethereum frameworku. V případě EIP 4361, tzv. „Sign in with Ethereum“ umožňuje využití Ethereum účtu ke správě své digitální identity. [7]

1.7.2 Hyperledger Foundation

Tato instituce je součástí Linux Foundation, kdy je jejím cílem poskytovat otevřené řešení týkající se DLT a blockchainových technologií. Jednotlivé projekty této organizace slouží jako stavební bloky pro vytváření produkčních blockchainových řešení. [8]

Hyperledger Fabric

Hyperledger Fabric slouží jako základní stavební kámen ve vytváření blockchain technologií specifických především pro průmyslové využití (např. v logistice). Jedná se o privátní řešení blockchainu, které nabízí jednotlivé moduly k vytvoření robustních blockchainových řešení. Fabric podporuje také variaci smart kontraktů, známou jako chaincode. Daný chaincode je možné psát v různých programovacích jazycích. [8]

Hyperledger Ursa

Ursa poskytuje kryptografické knihovny pro využití v ostatních aplikacích. Například v případě Hyperledger Indy či Aries obsahují knihovny pro:

- generování klíčových párů (veřejných a privátních)
- šifrování a dešifrování dat
- podepisování a ověřování dat
- hashování dat a jejich ověřování
- Zero knowledge proof (ZKP) knihovny, pro vydávání a revokování ZKP credentials a generování a ověřování ZKP [9]

Hyperledger Besu

Jedná se o open source Ethereum klienta, který se připojuje k Ethereum síti, nicméně může být nezávislý na blockchainové síti.

Ostatní

Součástí Hyperledger projektů jsou také identity řešení Hyperledger Indy, Hyperledger Aries a Hyperledger AnonCreds, které jsou využity v praktické části. Veškerý popis komponent je uveden v kapitole 5.

1.7.3 IOTA

IOTA je velmi specifické decentralizované řešení, není totiž založeno na blockchainové technologii používající na sebe navazující řetězce bloků pro uložení dat. Namísto bloků využívá řízené acyklické grafy tzv. Tangle. Uvedený framework je využitelný především pro IoT aplikace, kdy není potřeba obrovské výpočetní prostředky, ale zato je důležitá škálovatelnost a propustnost sítě.

IOTA postoupila také na poli decentralizované identity, kdy poskytuje možnost využití identity frameworku programovaného v Rustu. [10]

1.7.4 ION Network

Jedná se o řešení decentralizované identity od firmy Microsoft běžící na druhé vrstvě bitcoin blockchainu. ION nabízí identity framework se svými vlastními Azure AD verifiable credentials, OpenID autentifikaci a vlastní DID (decentralizovaný identifikátor) metodu. ION protokol byl standardizovaný v rámci Identity foundation, která má za cíl vytvářet standardy na poli decentralizované identity. [11]

1.7.5 Polygon

V březnu 2023 blockchainová síť polygon oznámila implementaci tzv. Polygon ID. Jedná se o implementaci a podporu všech self sovereign identity komponent v rámci polygon networku. Polygon má svou vlastní DID metodu pro rozlišování svých DID dokumentů. DID dokumenty jsou detailně popsány v kapitole 2.8. [12]

1.8 NFT a SBT

NFT (Non-fungible token) jsou unikátní identifikátory zaznamenané na blockchainu a jsou používány pro ověřování vlastnictví. Jsou tedy z podstaty věci neměnné, nicméně podporují možnost přesunu z jednoho vlastníka na druhého. Z pohledu identity se tedy NFT jeví jako neaplikovatelné. Identita z pohledu fyzického světa není obchodovatelná. Delegace identity je sice možná, ale v rámci NFT dochází k převodu vlastnictví na jinou entitu.

Soulbound token tzv. SBT jsou velmi podobné svými vlastnostmi NFT nicméně nejsou převoditelné. Jsou vztaženy k vlastníkovi. [13]

2 IDENTITA

Definice termínu identita může být velice subjektivní ve spojitosti s kontextem ke kterému se termín identita vztahuje, nicméně podle Cambridge slovníku:

„Jméno osoby a další fakta o tom, kdo daná osoba je."

„Fakt o existenci, pocitu o sobě samém, specifický typ osoby či organizace, vlastnostmi, co dělají osobu, organizaci odlišnou od ostatních." [14]

National Insitute of Standards and Technology (NIST) obsahuje z pohledu identity v digitálním světě směrodatnější definice a to konkrétně:

„Sada fyzických a behaviorálních charakteristik, kterými je osoba unikátně rozpoznatelná." [15]

2.1 Digitální identita

Digitální identitu lze specifikovat jako onlinovou či síťovou identitu akceptovanou či nárokovanou jednotlivcem, organizací nebo elektronickým zařízením v kyberprostoru. Tyto entity mohou vlastnit více než jednu digitální identitu prostřednictvím více organizací. V rámci správy digitální identity jsou hlavními zájmovými oblastmi bezpečnost a soukromí. [16] [17]

2.2 Modely ověřování identity

Uvedené modely představují základní paradigmata ve správě identity a údajů o jednotlivci či organizaci.

2.2.1 Centralizovaný

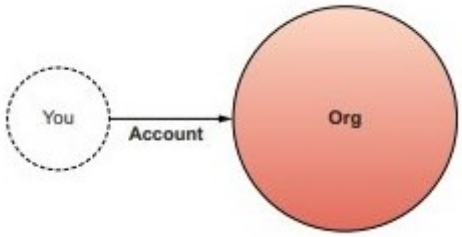
Centralizovaný přístup ke správě identit stále v prostředí internetu vystupuje jako dominující. Je charakteristický pro většinou známých vztahů mezi držitelem a organizací, která daný dokument vydává a ověřuje.

Z pohledu fyzických nosičů identity se jedná o pasy, občanské či řidičské průkazy, kdy jsou tyto dokumenty vydávány centrální autoritou. Z pohledu digitální identity můžeme uvést jako nejznámější příklad uživatelské jméno a heslo. Dále bude diskutována pouze část týkající se digitální identity.

Držiteli je propůjčen/vytvořen přístup k účtu, díky kterému může interagovat se systémem. Veškeré informace o účtu i účet jako takový vlastní provozovatel dané služby. Zneplatnění identity je možné provést vymazáním z centralizovaného systému vydavatele, nicméně tyto akce jsou ve správě provozovatele služby.

Centralizovaný systém má nedostatky nejen z pohledu běžného uživatele, ale i z pohledu provozovatele služby. Provozovatel totiž musí zajistit odpovídající aplikaci zabezpečení dané identity, případně musí zvládat další vrstvy autentifikace např. MFA (Multi Factor Authentication). Zároveň musí udržovat aplikační logiku autentizace pro služby na své straně a tím pádem jsou zde požadavky na pravidelné opravy bezpečnostních hrozeb. [18]

Z pohledu bezpečnosti existuje u tohoto typu zvýšený risk krádeže osobních informací, pokud nejsou dostatečně zabezpečena. Uživatel musí pro každou službu použít nové identifikátory, kterými se může autentizovat. Z toho vyplívající nutnost spravovat více uživatelských účtu a nejlépe využití externích aplikací pro správu hesel (tzv. Password managery). Nicméně tyto služby nejsou u všech uživatelů standardem a při využití stejného hesla na více webech riskuje uživatel možnost ztráty uživatelských účtů, případně i finanční ztrátu. [17]



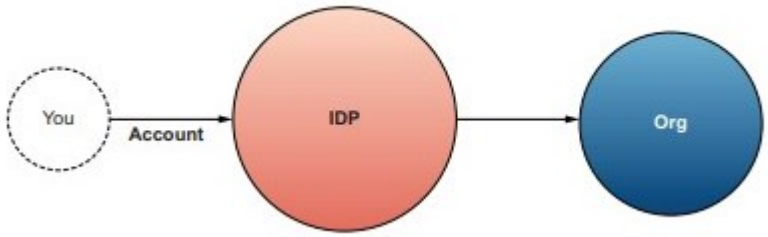
Obrázek 4. Centralizovaná identita [18]

2.2.2 Federovaný

Federovaný model identity obsahuje z pohledu fungování tři mandatorní entity.

- Uživatele
- Organizaci či službu, kterou daný uživatel využívá, tzv. relying party (RP)
- Identity provider (IDP)

Uživatel vlastní pouze jeden účet v rámci IDP, který využívá k přihlašování k organizacím, využívající těchto služeb, využívá tím tzv. mechanismus „Single sign-on“ (SSO).



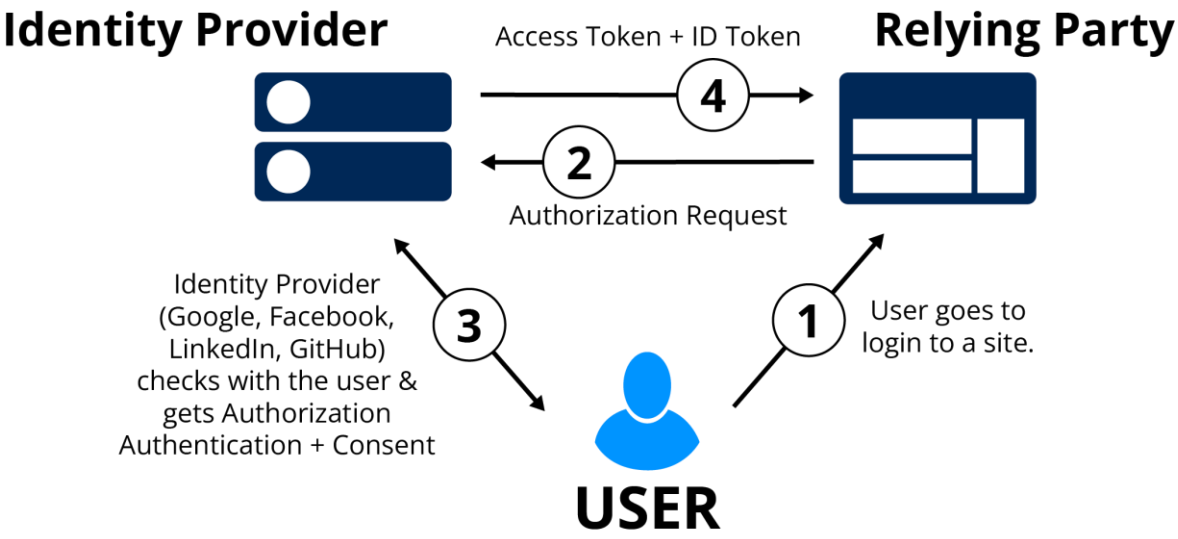
Obrázek 5. Role IDP ve federované identitě [18]

Výhodou federované identity je především využití autentizace IDP u nedůvěryhodných služeb, kde se obáváme ukládat všechny nutné údaje. (Pozn. IDP přesto poskytuje určitý obsah údajů s kterými je nicméně potřeba souhlasit). Nicméně i federovaná identita obsahuje nedostatky, které mohou být potencionálně nevýhodné pro uživatele. V případě IDP je nám propůjčována identita prostřednictvím IDP služeb, kdy kompletní kontrolu nad uživatelskými daty vlastní provozovatel IDP. Zároveň jsou tyto služby obsahují větší riziko z pohledu honeypotů pro potenctionální hackerské útoky. [18]

Existují tři protokoly, které byly vyvinuty pro služby FIM (federovaného identity managementu). [19]

- SAML
- OAuth
- OpenID connect

V České republice poskytují FIM v rámci elektronické identity MojeID, která je využitelná napříč českými institucemi a je spolu s Bankovní identitou, případně NIA ID (Národní identitní autorita) využitelnou i pro interakci s aplikacemi státní správy. [20] Další ukázkou federované identity je i SSO služba Shibboleth využívaná Univerzitou Tomáše Bati.

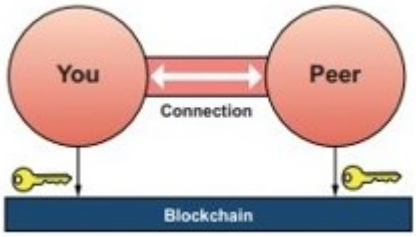


Obrázek 6. Proces ověření pro federovanou identitu [17]

2.2.3 Decentralizovaný model

Původní decentralizovaný model pochází z tzv. Fast Identity Online (FIDO) modelu, kdy jsou mezi účastníky navázány P2P spojení, ale management klíčů je prováděn centralizovaně u organizace tzv. FIDO aliance.

V rámci decentralizovaného modelu nevlastníme žádný účet u IDP ani u poskytovale služby. V uvedeném modelu, tím že se jedná o simulaci reálného světa, navazujeme vztahy a důvěru mezi jednotlivými entitami, v tomto případě peery. V P2P vztahu nevlastní ani jedna entita účet ale sdílí se spojení mezi sebou. V průběhu výměny si entity vymění kryptografický materiál, tzn. veřejné klíče a decentralizované identifikátory za účelem navázání bezpečného a soukromého spojení. Tyto vlastnosti poukazují na skutečnost chybějící centrální certifikační autority, která by řešil správu veřejných klíčů. V kontextu decentralizovaného modelu se nabízí termín decentralizovaná infrastruktura veřejných klíčů (Decentralized Public Key Infrastucture – dále DPKI. Zároveň dochází k ukládání některých z těchto veřejných klíčů na DLT veřejného blockchainu. Slouží primárně k ověření podpisu v případě verifiable credentials (VC), tak aby bylo možné ověřit důkaz v rámci SSI. [18]



Obrázek 7. Decentralizovaná identita [18]

2.3 Zákony identity

Kim Cameron definoval již v roce 2005 sedm zákonů identity, které využívaly organizace po celém světě při implementaci identity systémů:

- Uživatelská kontrola a souhlas – systém může odhalit jen ty informace které mohou identifikovat uživatele výhradně se souhlasem uživatele
- Omezené použití s minimálními zveřejněním informací – pro dlouhotrvající řešení je nejlepší snížit počet sdílených informací na minimum
- Oprávnění účastníci – zveřejňování informací by mělo být v rámci digitální identity nejlépe pouze organizacím se kterými má identity systém navázán speciální vztah
- Řízená identita – univerzální identity systém by měl používat jak veřejné identifikátory, tak i jednosměrné identifikátory pro privátní použití, což usnadní zjišťování a zároveň zabrání korelaci identifikátorů
- Pluralita provozovatelů a technologií – obecně se jedná o interoperabilitu mezi jednotlivými provozovateli identit používající jiné technologie
- Integrace člověka – člověk musí být součástí distribuovaného systému při komunikaci mezi člověkem a systémem, a tím se zabezpečí proti potencionálním útokům
- Konzistentní zkušenost v různých kontextech – sjednocený systém identit musí poskytnout jednoduchou a konzistentní zkušenost [21]

2.4 Kryptografie

Kryptografie využívaná pro potřeby decentralizované identity zahrnuje i funkce hashování a asymetrickou kryptografii. Z důvodu fungování systému založeném na asymetrický kryptografii je nutné tyto nástroje spravovat v rámci bezpečného, a především důvěryhodného ekosystému.

2.4.1 PKI vs. DPKI

Public Key Infrastructure (PKI) je sada nástrojů a procesů (hardwaru, softwaru, pravidel, procesů a procedur), které jsou nutné pro tvorbu, správu, distribuci, použití, uložení a zneplatnění digitálních certifikátů a veřejných klíčů. PKI je základem pro využití technologií založených na kryptografii, např. digitální podpisy, šifrování dat ve větších měřítcích. PKI jako řešení poskytuje důvěru v bezpečnost daného ekosystému. [22]

DPKI je alternativní přístup ke správě infrastruktury veřejných klíčů, kdy není třeba žádné centrální autority, která v PKI slouží k podepisování certifikátů. Jednotlivé entity v rámci blockchainu mají možnost nativně zjistit poslední verzi veřejného klíče a mohou být tedy správci svých vlastních certifikátů. [23]

2.4.2 ZKP

Zero Knowledge Proof je typ kryptografické metody při které musí tzv. dokazovatel (prover) dokázat tzv. ověřovateli (verifier), že vlastní určitou část informace bez odhalení samotné informace.

Metoda musí splňovat tyto charakteristické vlastnosti:

- Úplnost – v případě že je důkaz pravdivý a dokazovatel i ověřovatel dodržují pravidla protokolu, pak může ověřovatel potvrdit důkaz bez jakékoliv pomoci třetí strany.
- Znělost (Soundness) – pokud ověřovatel není přesvědčen pak může označit důkaz za nepravdivý, nicméně pravděpodobnost chybného vyhodnocení metody se pravděpodobnostně blíží nule.
- Zero knowledge (Nulová znalost) – Ověřovatel se nedozví žádné další informace. [24]

Interaktivní

Interaktivní ZKP je typ ZKP, kdy dochází k výměně zpráv/interakce mezi dokazovatelem a ověřovatelem. Dokazovatel během této interakce odpovídá na dotazy ověřovatele. Během interakce dochází k několika iteracím pokládání dotazu. Tato metoda je velmi časově i výpočetně náročná, a proto se nevyužívá v produkčních systémech tak jako neinteraktivní ZKP.

Neinteraktivní

U neinteraktivních ZKP proběhne odeslání důkazu prokazovatelem pouze jednou, a to bez nutnosti ověřovatele se zpětně dotázat. Z pohledu aplikační logiky tato možnost nepožaduje, aby byly obě entity online pro výměnu dotazů. Nejznámější implementace neinteraktivních ZKP jsou aktuálně v roce 2023 zkSNARK (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) a zkSTARK (Zero-Knowledge Scalable Transparent Argument of Knowledge). První implementace zkSNARK byla vytvořena v roce 2014. Pro vytvoření důkazu je využito kombinace veřejného a privátního klíče. Prokazovatel použije privátní klíč pro vygenerování důkazu a ověřovatel využije veřejného klíče k ověření důkazu. Metoda zkSTARK byla představena v roce 2018, kdy používá jinou metodu oproti zkSNARK. V případě zkSTARK není nutné využití privátního klíče pro ověření pravdivosti tvrzení. Zároveň je uvedená metoda poskytuje důkazy ověřit daleko rychleji, díky exponenciálnímu škálování, a to vzhledem k množině dat, kterou reprezentují. [24][25]

2.5 SSI

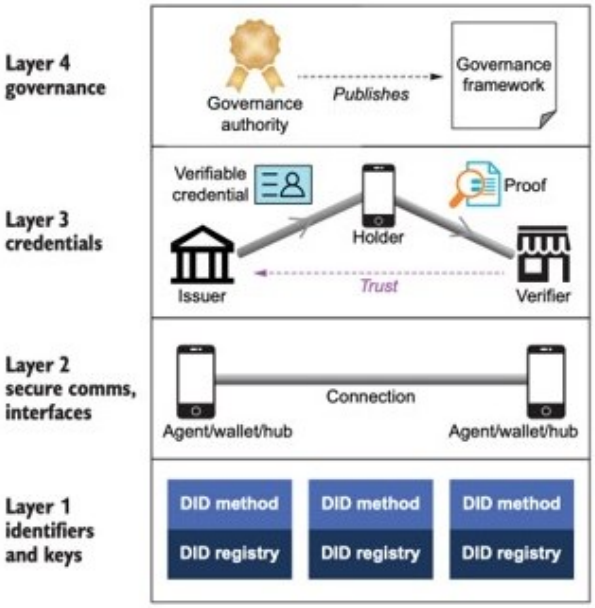
Self sovereign identity je framework pro vytvoření decentralizované identity. Jednotlivé části jsou definovány pomocí čtyřvrstvého paradigmatu vydaného komunitou Hyperledger Aries v roce 2019. Spodní dvě vrstvy jsou především o dosažení technické důvěryhodnosti

a horní dvě vrstvy se týkají spíše dosažení lidské důvěry. Lze konstatovat fakt, že SSI jak i vlastně ostatní identity frameworky závisí na důvěře v daný systém.

Viz. Obrázek č. 8 první vrstva je souborem identifikátorů a metod, používané k zajištění důvěry mezi všemi uživateli SSI. Nicméně aby tyto identifikátory mohly být považovány za důvěryhodné, je třeba zajistit důvěru, která je v aktuálních řešeních zajištěna tzv. VDR (Verifiable data registry). Na VDR jsou uloženy jak informace o uvedených identifikátorech a schématech, tak i veřejné klíče. Nástup technologie blockchain zajistil tuto vrstvu důvěryhodnosti, nicméně z obecného hlediska může být VDR i jiná sdílená databáze, pokud je pro všechny účastníky důvěryhodná.

Druhá vrstva je o vytvoření zabezpečené komunikace mezi dvěma entitami pomocí TLS a specifických TCP/IP protokolů. Může to být instituce nebo i jednotlivec, či digitální peněženka v serverové či klientské podobě.

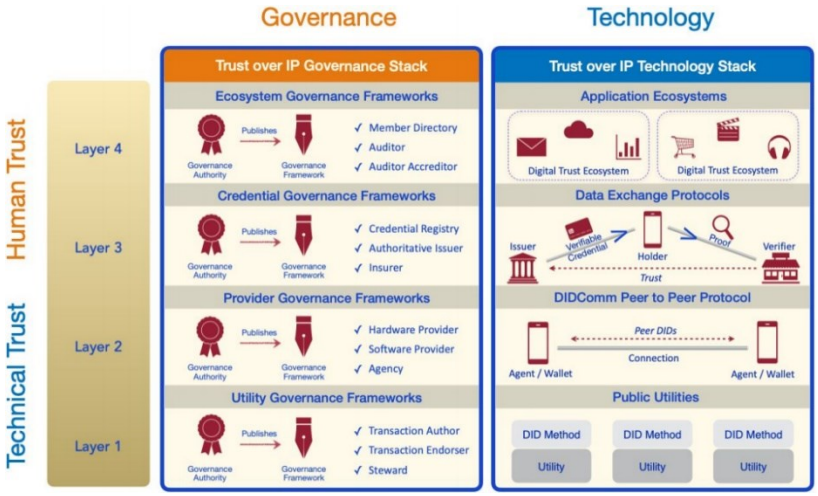
Třetí vrstva SSI se týká procesů v rámci vydávání identifikátorů (Verifiable credentials), kdy musí být definovány nejen formáty daných identifikátorů, ale především musí být dány i způsoby, jak identity vydat, jak je zabezpečit a jak je zpracovat. Jedná se tedy spíše o technickou vrstvu daného frameworku s důrazem na důvěru prostřednictvím kryptografie. Nicméně v kombinaci s vrstvou 4, která je spíše zaměřena na procesy a nastavení důvěry mezi jednotlivými účastníky v rámci systému. Je řešeno, zde několik důležitých prvků, jak nastolit v celém ekosystému důvěru na základě limitů. jak probíhá uložení dokladů, a především jak nastavit důvěru mezi jednotlivými účastníky, tak aby ověřovatel mohl důvěřovat vydavateli identity. Tyto vztahy navazují na tzv. Trust Triangle, který bude popsán více v kapitole 2.6. [18]



Obrázek 8. Vrstvy SSI [18]

2.5.1 Trust over IP

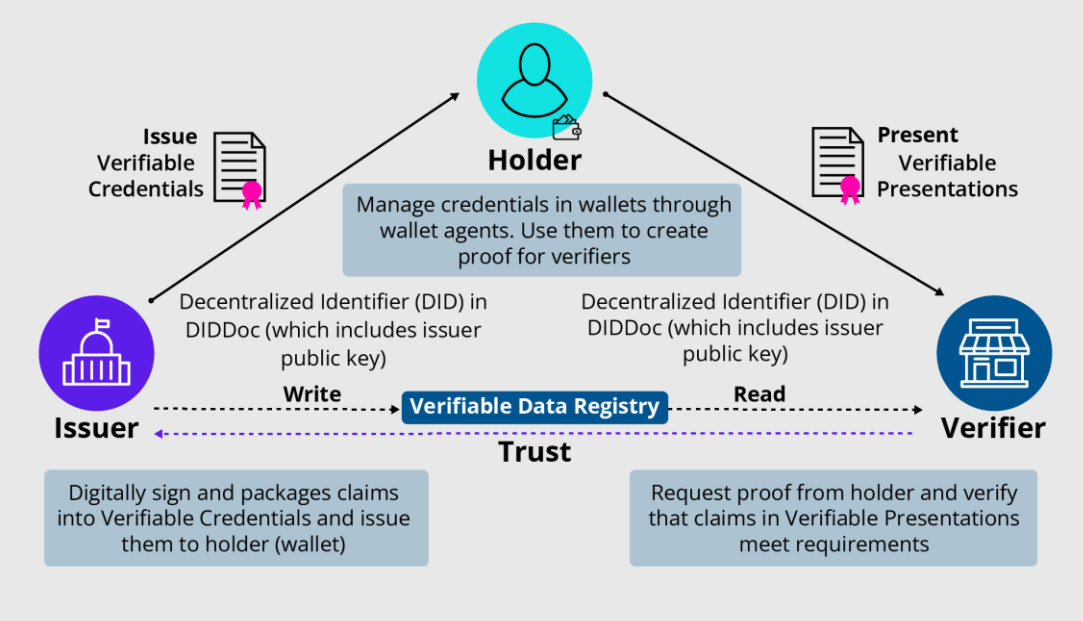
Trust over IP je soubor technických protokolů, který slouží jako framework pro nastolení důvěry mezi jednotlivými entitami v prostředí internetu. Přesně definuje všechny zainteresované strany SSI ekosystému a rozšiřuje SSI vrstvy o tzv. „governance framework“. Doslovně se jedná o rámec řízení. [18]



Obrázek 9. Trust over IP [9]

2.6 Trust triangle

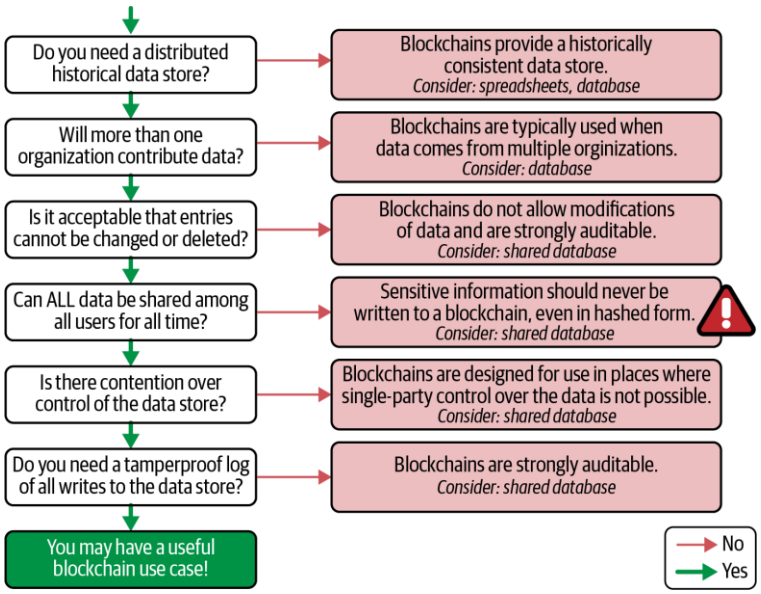
Proces vydávání a ověřování identity v rámci self sovereign identity je znám jako „trust triangle“. Definuje tři účastníky a jednu vrstvu důvěry. Výměna informací identity obecně potřebuje tři odlišné role a to vydavatele (Issuer), držitele identity (Holder) a ověřovatele (Verifier). Vydavatel na požadavek držitele identity vydává identitu a nabídne tuto identitu držitele k uložení. Pokud je vydavatel důvěryhodný, držitel poté může využít danou identitu pro přístup ke službám, které daná identita nabízí. Identitu jako držitele poté ověřovatel identity pomocí kryptografie ověří. [17]



Obrázek 10. Trust triangle [17]

2.7 VDR

Verifiable data registry (VDR) je tzv. vrstva důvěry na jejímž základě si může ověřovatel pomocí kryptografických metod ověřit, zda se prokazovatel (držitel) identity prokazuje údaji vydanými a podepsanými vydavatelem. Zároveň zde mohou být uloženy i veřejné klíče vydavatele, decentralizované identifikátory a další informace závisející na implementaci. VDR může být řešeno pomocí blockchainu, nicméně lze využít i jiná řešení, např. centralizované databáze. Závisí zde na požadavcích vlastnosti systému, kdy v některých případech využití blockchainu může být kontraproduktivní [17].



Obrázek 11. Vhodnost blockchainu jako VDR [26]

2.8 DID decentralizované identifikátory

DID je identifikátor, který umožňuje identifikovat entitu na internetu bez nutnosti použití centrální autority (např. státní správa, organizace). Nad svým DID máte plnou kontrolu a můžete ji využít i pro prokázání sebe samého. Zatímco centralizované identifikátory jsou využívána jako identifikátor pro využití služby a za které se považují např. jména a hesla. DID umožňuje jednotlivcům i organizacím generovat vlastní identifikátor využívající systémů kterým daná entita důvěřuje. Za pomocí kryptografie tedy umožňuje kontrolovat

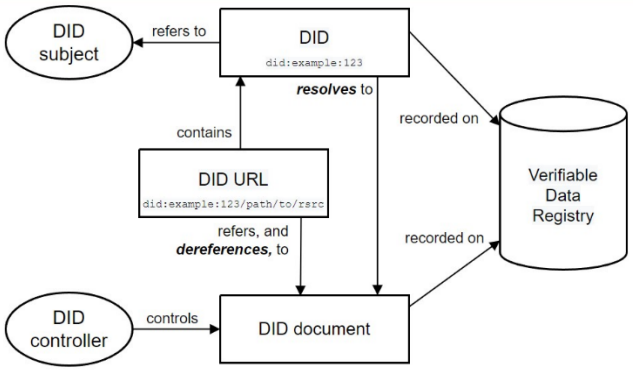
vlastní identifikátory. Organizace W3C (World Wide Web Consortium) vytvořila standard pro strukturu DID v červenci 2022 ve verzi 1.0. [27][28]

2.8.1 Vlastnosti

DID se od ostatních URI identifikátorů liší čtyřmi zásadními prvky a z toho důvodu má i svůj vlastní standard zmíněný výše.

Konkrétně se jedná o tyto vlastnosti:

- Permanentní – DID jsou z povahy věci permanentní identifikátory a jejich návrh by měl počítat s dlouhodobou platností
- Rozlišitelná – DID jsou rozlišitelné identifikátory, uživatelé tedy mohou najít informace, jak ke každému DID dokumentu přistoupit
- Kryptograficky ověřitelná – každý uživatel by měl mít možnost pomocí veřejného klíče ověřit validitu DID dokumentu
- Decentralizovaná – DID je využitelný především v decentralizovaných databázích mimo dosah centralizovaných autorit [29]



Obrázek 12. Složení a popis DID [27]

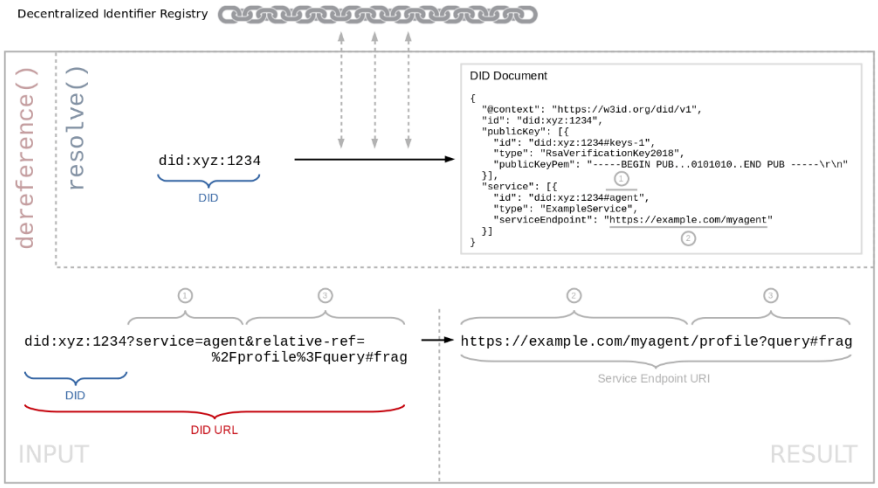
2.8.2 Rozlišování DID

Rozlišování DID probíhá prostřednictvím dereferencování DID URL procesem načtení reprezentace zdroje z DID URL pomocí softwaru či hardwaru. Proces, který tento krok provádí se nazývá „DID resolver“. Hranice pojmu „resolving“ a „dereferencing“ jsou stále předmětem diskuzí v kontextu DID.

Na uvedeném příkladu Obrázku 11. bude popsáno dereferencování DID dokumentu „did:xyz:1234“.

DID se skládá z několika částí:

- Schématu – hodnota „did“
- Metody – hodnoty „xyz“, obecně existuje vysoký počet DID metod, nicméně tyto metody musí splňovat standardy W3C a až poté dojde k jejich veřejnému uveřejnění v dokumentacích W3C
- Specifický identifikátor DID dokumentu – „1234“, obecně se může například o adresu peněženky, identifikátor agenta pro spojení mezi agenty, aj. [30]



Obrázek 13. Dereferencování DID [30]

2.8.3 Metody DID

Jednotlivé metody DID obsahují specifické vlastnosti dané metody, mají vlastní dokumentaci po schválení implementace uvedeného DID je nová metoda na webu W3C.

DID:Web - Jedná se o standardní DNS architekturu charakteristickou pro web 1.0 a 2.0. díky čemu je zachována zpětná kompatibilita.

DID:Peer – je vhodný pro většinu soukromých vztahů mezi lidmi, organizacemi a věcmi. Vytváří podmínky pro to, aby lidé, organizace a věci měli plnou kontrolu nad svou částí digitálních vztahů, které udržují. Převážně se používá na navázání spojení mezi jednotlivými agenty. Nicméně vzhledem k rychlému vývoji na poli DID, je doporučeno migrovat na DID:keri, případně na DID:key, závisející od implementace. Nicméně DID:peer je stále nativní pro projekt hyperledger Aries pro komunikaci agentů mezi sebou.

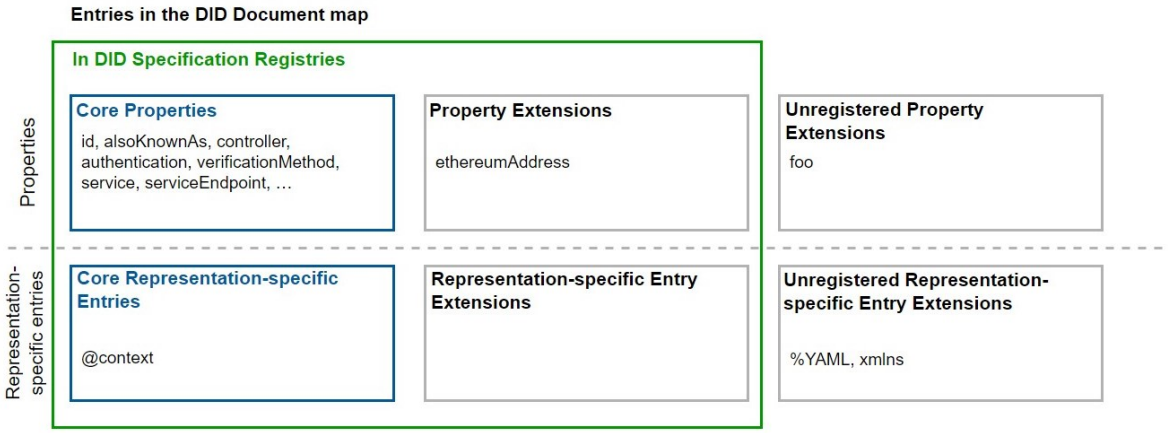
DID:indy – jedná se o DID metodu specifickou pro Hyperledger Indy blockchain framework, která umožňuje interakci s jednotlivými objekty na blockchainu.

DID:Key - se používá k vyjádření veřejných klíčů způsobem, který nevyžaduje žádný registr DID. Jedná se o off-line přívětivou, kryptograficky samo certifikační metodu, která nevyžaduje důvěru certifikačních autorit ani blockchainu a je ideální pro efemérní použití. [31]

DID:keri – jedná se o metodu, která umožňuje rotaci klíčů v decentralizovaných sítích na základě tzv. „key event logu“. Což je datová struktura zřetězených hashů, z kterých je možné odvodit stav klíče specifického keri identifikátoru. [32]

2.8.4 Datový model

Datový model DID dokumentu se skládá z „mapy“ záznamů, kde každý záznam obsahuje klíč a hodnotu. Datový model by měl obsahovat alespoň dvě různé třídy záznamů. První třída záznamů by měly být tzv. Core Properties a druhá třída tzv. representation specific entry extensions. [27]



Obrázek 14. DID datovy model [27]

2.8.5 DID Comm

Jedná se o standard komunikace mezi jednotlivými agenty pro decentralizované identity systémy, které jsou založené na DID. Vytváří bezpečný komunikační kanál mezi jednotlivými agenty. Komunikace mezi agenty je zabezpečena pomocí kryptografie. Nejedná se o komunikaci mezi klientem a centrálním serverem, ale o P2P spojení mezi dvěma entitami. [33]

2.9 Verifiable credentials

Verifiable credentials (VC) je digitální dokument založený na open standardech W3C. Tento dokument dokáže reprezentovat informace z reálného světa i fyzických dokumentů (pasy,

ŘP). V porovnání s fyzickými dokumenty obsahují možnost vyjádřit i data, která by byla velmi složitě prezentovatelná v rámci fyzického nosiče. Např. detaily o zdravotním stavu, detaily vlastníka účtu, všechny dosažitelné kvalifikace aj. Standardně na fyzický dokument obsahuje informací identifikující předmět či účel vydaného dokumentu, identifikaci vydavatele, specifické atributy dle účelu dokumentu, evidenci o vytvoření dokumentu, případně i omezení dokumentu (datum exspirace, podmínky použití dokumentu). VC všechny tyto parametry dokáže reprezentovat. [34]

Verifiable credentials se skládají ze tří základních komponent:

- Metadat
- Tvrzení, tzv. claims
- Důkazu, tzv. proofs

2.9.1 Metadata

Metadata specifikují, v jakém formátu jsou dané VC prezentovány, v případě W3C VC verze 1.1 obsahují tyto pole:

- **@context –** poukazuje v jakém formátu je dokument zakódován. Jednotlivé formáty VC budou specifikovány v následující kapitole 2.9.5.
- **type** – specifikace typu VC, může specifikovat obecně VerifiableCredentials, a poté specifický typ danému dokumentu
- **id** – reference na unikátní záznam dokumentu
- **issuer** – unikátní identifikátor issuera, může se jednat o DNS záznam issuera případně did dokument či registr, kde je uložen veřejný klíč issuera [18]

2.9.2 Claims

Tvrzení označuje informace, které o sobě subjekt tvrdí a snaží se je prokázat. Je možné si je představit jako jednotlivé atributy subjektu např. jméno a příjmení, datum narození, adresa aj. Tyto informace jsou uloženy v digitální peněžence subjektu. Z pohledu fyzických dokumentů se jedná např. v případě občanské průkazu o všechny atributy charakterizující osobu. Pravdivost tvrzení je poté ověřována pomocí důkazů. [26]

V rámci W3C VC se jedná o pole credentialSubject s hodnotami všech tvrzení, které mají být porovnávány ve formátu (klíč: hodnota). V rámci tvrzení mohou být porovnávány hodnoty, které nejsou žádoucí pro sdílení s ověřovatelem (citlivé údaje, např. datum narození)

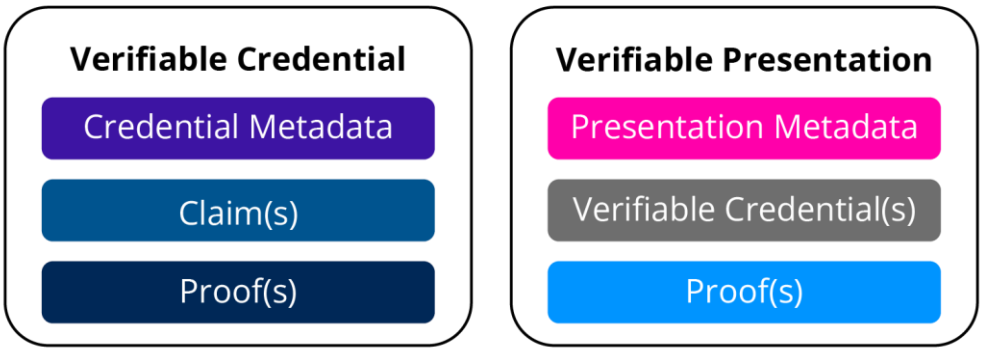
a je nutné pouze ověřit, zda subjekt je starší než osmnáct let. Jedná o tzv. selektivní zpřístupnění informací, kdy je využito ZKP. [18]

2.9.3 Proofs

Důkazem lze dokázat, zda jsou tvrzení subjektu či osoby správná. V reálném světě se jedná o bezpečností prvky např. občanského průkazu. V případě VC jsou tyto důkazy založeny na kryptografii, kdy vydaný dokument je v průběhu vydání dokumentu podepsán. A poté je pomocí veřejného klíče ověřen a že nedošlo k nedovolené úpravě dat. [18]

2.9.4 Verifiable presentation

Verifiable presentation (VP) reprezentuje data získané z jednoho nebo více VC. VC jako takové mohou být beze změny prezentovány jako VP. VP můžou obsahovat i data která jsou derivovaná z VC či data z více VC najednou. nicméně obvyklý scénář je ten že VP a předmětné VC v rámci VP jsou totožné. Je nutné podotknout, že v případě že se prezentace skládá z více VC, tak musí být podepsán jednotlivě svým vydavatelem dokumentu. [35] [36]



Obrázek 15. Komponenty VC vs VP [35]

2.9.5 Formáty VC

W3C VC

Aktuálně existuje W3C datový model verifiable credentials v 1.1 finalizovaný v březnu 2022. Jeho parametry byly uvedeny již v kapitole 3.10. Aktuálně probíhá standardizace nové verze VC 2.0., která je nicméně stále vedená jako pracovní. [34]

AnnoCreds

Původně byl tento formát VC funkční pouze s blockchainovým frameworkem Hyperledger Indy, nicméně nyní se již jedná o nezávislý formát VC na jakémkoliv VDR. Musí splňovat požadavky, které AnonCreds vyžaduje aby byly ukládány na VDR. AnonCreds umožňuje práci s dokumenty v rámci celého „Trust triangle“, poskytuje tedy VC, VP i tzv. multidokumenty (multicredentials). Podporuje také atributy se selektivním zpřístupněním informacím pomocí ZKP. [37]

Mobile Driver License

Jak již anglický název napovídá jedná se o specifický typ mobilní dokumentů pro řidičské průkazy. ISO organizace má již od začátku 21. století pracování skupinu pro standardizaci řidičských průkazů, v roce 2018 tedy tato pracovní skupina vydala ISO 18013-5, který definoval mobilní řidičské průkazy. V únoru 2023 nicméně byl vydán další standard ISO/EIC 23220-1:2023, který specifikuje architekturu i procesy pro mobilní eID systémy. Obecně se ale tento formát nepovažuje vhodný pro implementaci SSI systému, kdy se uvažuje spíše na interoperabilitě s W3C VC. [38] [39]

2.10 Digitální peněženky

Tak jako v reálném světě jsou využívány peněženky pro nošení peněz, tak jsou také využívány k držení dokladů, kterými se v případě potřeby můžeme prokázat. V digitálním světě nyní existují tři typy peněženek.

- Mobilní peněženky pro placení emulovanými platebními kartami (např. Apple Pay, Google pay) s možností uložení letenek či benefitních karet
- Kryptoměnové peněženky pro uložení kryptoměn a tokenů (např. Trezor Wallet)
- Digitální peněženky pro svých digitálních identit

V rámci peněženky pro identitu je nicméně nutné brát na zřetel, že se jejich implementace týkají především centralizovaných řešení pro státní aparát. Např. digitální ID karty v Estonsku, i-Pin ID card řešení v Jižní Korei a další. [40]

2.10.1 Specifikace peněženek

Peněženky pro digitální identitu lze rozčlenit na peněženky serverové a klientské. Obecně jsou všechny peněženky známé pod termínem agenti. Agenti jsou software, který je uzpůsobený pro práci s DID a VC. Zároveň agenti udržují spojení/vztahy mezi ostatními agenty

s kterými jsou propojeni. Peněženky mohou obsahovat i informace nerelevantní ke standardům digitální identity, nicméně relevantní ve vztahu k identitě, kterou reprezentují (např. PDF fyzického dokumentu, jména hesla, vlastní VC). [18][26]

Serverové si můžeme představit jako zabezpečenou databázi či spíše uložiště obsahující všechny DID, klíče a VC. Vesměs tedy všechny identifikátory nutné pro SSI identity systém. Tento systém může běžet ve standardním datacentru či v cloudu. [9]

3 EVROPSKÁ UNIE A SSI

3.1 EIDAS

V roce 2014 byla vydána první verze nařízení EIDAS. Jednalo se o první legální nástroj pro důvěryhodnost služeb digitální transakce. EIDAS vydal legislativní rámec a regulace pro práci s elektronickými podpisy a dalšími důvěryhodnými autentizačními metodami. Zároveň nařízení vyžaduje interoperabilitu mezi státy EU.

Tímto nařízením tedy vznikly standardy pro elektronické podpisy, elektronické dokumenty. kvalifikované digitální certifikáty, elektronické pečeti a časová razítka. [41]

3.2 EIDAS 2

EIDAS 2 je návrh nařízení Evropské unie, který řeší nedostatky nařízení EIDAS z roku 2014 a nabízí legislativní rámec pro digitální identitu. Finální verze návrhu byla vytvořena v červnu 2021. S nařízením EIDAS 2 přichází požadavek na zvýšení bezpečnosti nejen z pohledu provádění transakcí, smluv jako v případě EIDAS 1 ale i evropské digitální identity. EIDAS 1 totiž neřešení poskytování elektronických identifikátoru či atributů jako jsou zdravotní data, kvalifikaci. Jedním z cílů EIDAS 2 je tedy vytvořit komplexní evropskou digitální identitu, která je interoperabilní mezi jednotlivými členskými státy a to prostřednictvím tzv. Evropské digitální peněženky a zároveň tomuto řešení poskytnout plný legislativní rámec. V roce 2024 musí dle nařízení EU všechny členské státy poskytnout digitální peněženku identity pro každého občana, pokud bude chtít. Tzv. EUDI (European Identity Wallet).

EUDI Wallet bude v souladu s nařízením GDPR a Cyber Security Act. Být interoperabilní s možností selektivního zveřejňování informací (např. věk). Aktuálně je známá podpora online identifikace identity a využití elektronických podpisů. [41][42]

3.3 GDPR

GDPR (General Data Protection Regulation) je nařízení Evropské unie, které se zabývá ochranou osobních údajů občanů EU a EHP (Evropského hospodářského prostoru). Toto nařízení bylo přijato v roce 2016 a nabylo účinnosti od 25. května 2018. GDPR obecně poskytuje občanům Evropské unie větší kontrolu nad tím, jak jsou jejich osobní údaje zpracovávána. Nařízení stanovuje řadu povinností pro organizace, které zpracovávají osobní údaje,

a to především zajistit odpovídající bezpečnostní opatření pro ochranu osobních údajů a povinnost informovat jednotlivce o tom, jak jsou jejich údaje používány.

Zásady GDPR zahrnují několik práv občanů:

- právo být informován
- právo na přístup
- právo na opravu osobních údajů
- právo na výmaz
- právo na omezení zpracování
- právo na přenositelnost údajů [43]

3.3.1 MiCA

Regulace MiCa (Markets in Crypto-Assets Regulation) se oproti jiným zmíněným legislativním dokumentům zabývá především regulací kryptoměn v rámci Evropské unie. Cílem je poskytnout legislativní rámec pro krypto aktiva, což zahrnuje decentralizované finance (tzv. De-Fi) tak i NFT. Vydavatelé a poskytovatelé těchto aktiv budou v rámci evropské unie poskytovat služby s ohledem na tento legislativní rámec. Poslední část MiCa se zabývá vytvoření specifických pravidel pro poskytování stablecoinů, což může být počátek legalizace elektronických peněz. [44]

3.4 Inicitava ESSIF

ESSIF (The European Self-Sovereign Identity Framework Lab) byl projekt Evropské unie spuštěný v roce 2020 s předem definovaným cílem, a to za pomocí SSI principů vytvořit inovativní návrhy pro využití decentralizované identity. Projekt poskytl prostředky pro vytvoření komunitních skupin pro standardizaci decentralizovaných identifikátoru (DID), verifiable credentials, projektů Hyperledgeru (Aries, Indy a Ursa). Díky ESSIF byla založena i tzv. DIF (Decentralized Identity Foundation) a Trust over IP foundation, která využívají všechny zmíněné komponenty k vytvoření moderního ekosystému SSI. V prosinci 2022 proběhl v rámci ESSIF finální konference, která měla za účel vyhlásit úspěšné dokončené inovace jak na poli řešení infrastruktury, tak na nových návrzích z pohledu business logiky SSI. Celková dotace vybraných projektů činila 5,6 milionu eur. [45]

3.5 EBSI

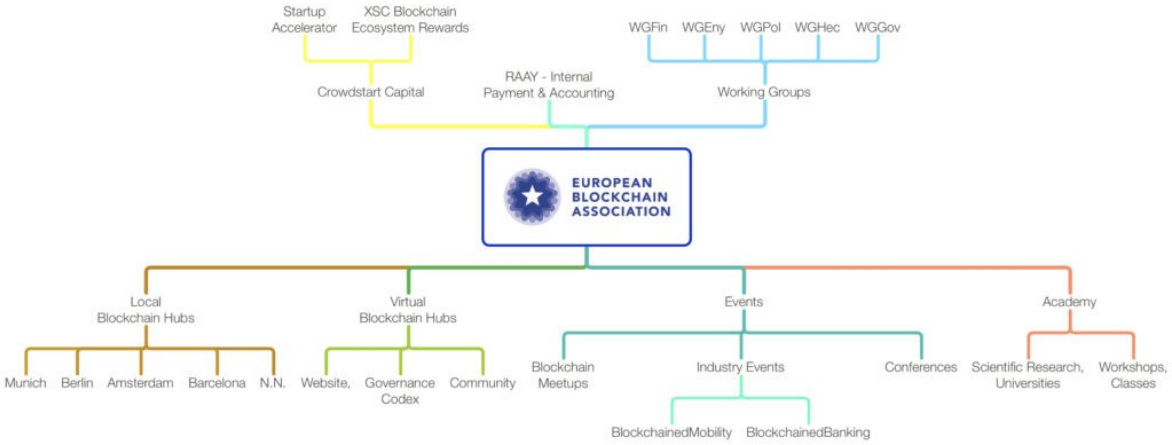
EBSI (European Blockchain Services Infrastructure) je iniciativa Evropské unie, konkrétně Evropské Komise a EBP (European Blockchain Partnership). Od roku 2020 organizace postupně nasazuje blockchainové nody po celé Evropě. Organizace má za úkol v dlouhodobém horizontu poskytovat služby týkající se digitální identity mezi které patří notářské ověřování dokumentů, osvědčení o vzdělání, vytváření digitálních identit, sdílení zdravotnických záznamů. Obecně Evropská unie cílí k tomu, aby byla na poli identity blockchainové infrastruktury v čele vývoje nejnovější trendů. [46]

3.5.1 Časová osa

Vývoj EBSI a jejich komponent je rozdělený na několik fází, z nichž některé jsou již ukončeny. V roce 2019 byl vyhlášen tendr Evropské unie na poskytnutí přeshraničního řešení využívajícího blockchainové technologie s ohledem na bezpečnost a ochranu osobních údajů. Fáze 1 byla v červnu 2021 po dobu třech měsíců, kdyby po splnění vyhodnocovacích kritérií do další fáze (2A). Tato fáze trvala šest měsíců a trvala od prosince 2021 do června 2022 a jednalo se především o vytvoření prototypů blockchainového řešení. V následující fázi 2B byly vybrány firmy. Aktuálně v roce 2023 probíhá pilotní testování a vývoj řešení dle požadavků Evropské unie. Do nejužšího výběru se dostaly firmy IOTA, BILLON a CHROMAWAY. [47] [48]

3.6 European blockchain association

EBA je tzv. DAO (Decentralizovaná autonomní organizace), která má za účel spojovat jedince a organizace v rámci blockchainových aktivit v Evropě. Její strukturu můžete najít na Obrázku č. 15. Členové EBA organizují přednášky v rámci blockchainových hubů a především se slučují v pracovních skupinách. EBA pracovní skupiny řeší konsenzuální algoritmy (tzv. Proof of Stake EUPoS), SSI pracovní skupina (EUSSI), tokenizační skupinu (EBA Tokenization) a další. [49]



Obrázek 16. EBA organizace a aktivity [49]

II. PRAKTICKÁ ČÁST

4 SCÉNÁŘ IMPLEMENTACE

Cílem praktické části práce je implementovat řešení pro vydání a ověření identity využívající vlastnosti blockchainu, a to bez nutnosti data sdílet a ukládat na serverech třetích stran. Důraz řešení je poskytnout možnost kontroly nad svou vlastní identitou. Tyto požadované vlastnosti systému vyžadují využití principů self sovereign identity.

V rámci praktické části budeme řešit situaci, kdy uživatel uzavřené internetové komunity, která v rámci svých pravidel vyžaduje věk starší než 18 let, bude mít možnost se přihlásit do svého účtu pomocí své vlastní identity. Prerekvizitou v uvedeném scénáři je nainstalovaná digitální peněženka podporující protokol uvedené implementace. Instalace a testy digitálních peněženek jsou uvedeny v kapitole 6.4. Další podmínkou je využití tzv. selektivního zpřístupnění informací, kdy při autentizaci uživatele nechceme sdílet skutečný věk uživatele. Chceme pouze potvrdit pravdivost informace o plnoletosti uživatele. Využijeme k tomu zero knowledge proof zvoleného frameworku.

Ve scénáři je počítáno s vytvořením a ověřením dvou identit jednotlivce. Prerekvizitou je vydání a uložení identity jednotlivce do digitální peněženky. Poté na základě této identity a ověření věku je umožněno vydání identity komunity, kterou je poté možné využít pro přihlášení do služeb komunity. Reálné využití bude diskutováno a popsáno v rámci evaluace implementace, a to i v kontextu případného napojení na EBSI z pohledu napojení vyvinutých agentů.

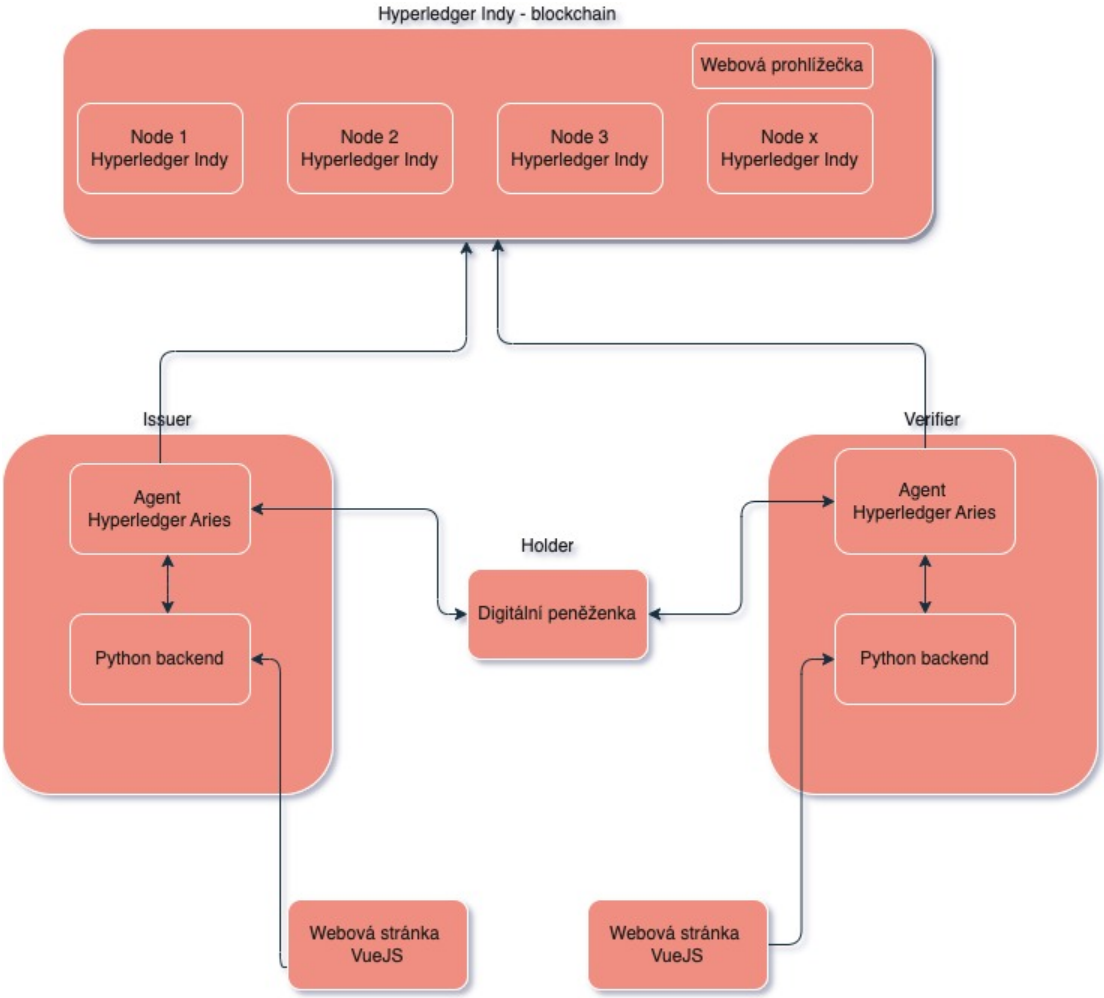
5 ARCHITEKTURA

Architektura decentralizované identity je definována vztahy mezi jednotlivými entitami, které budou vystupovat jako jednotliví účastníci daného systému. Řešení aplikuje tzv. trust triangle princip, který byl popsán v kapitole 3.6.

5.1 Cíle architektury identity

Navrhovaný identity systém se skládá z komponent, které budeme podrobně popisovat v následujících kapitolách a jednotlivě charakterizovat vlastnosti a konfiguraci, pro splnění cílů praktické části práce:

- Verifiable data registry (VDR)
- Agent pro komunikaci s držitelem identity a VDR s rolí vydavatele identity, tzv. „Issuer“, jedná se o vydavatele primární identity (ekvivalent státní instituce vydávající občanské průkazy)
- Agent pro komunikaci s držitelem identity VDR s rolí ověřovatele identity, tzv. „Verifier“, jedná se o agenta sekundární identity (komunity) s možností ověření primární identity
- Backendové systémy využívající SDK jednotlivých agentů se svou vlastní aplikační logikou
- Frontend, který zahrnuje aplikační logiku z pohledu uživatelského rozhraní systému
- Digitální peněženky



Obrázek 17. Jednotlivé komponenty řešeného systému [66]

5.2 VDR

Vrstvu důvěryhodnosti (VDR) zaštiťuje blockchainový framework Hyperledger Indy od společnosti Linux Foundations. Většina stávajících blockchainových řešení primárně cílí na využití v kryptoměnových aktivech, případně logistických aplikací pro lepší utilizaci dodavatelského řetězce. Projekt Hyperledger Indy byl vytvořen s cílem poskytnout nativně blockchainové řešení jako důvěryhodné vrstvy pro decentralizovanou identitu.

Pro případ vývoje je možné se připojit již ke stávajícím testovacím prostředím institucí, které vyvíjí své produkty nad blockchainem Hyperledger Indy. Prostředí, které by se dalo nazvat předprodukční, případně testovací, tak je možné využít veřejně dostupných sítí BCovrin, případně Sovrin nebo Indicio.[51]

Z pohledu vývoje svých vlastních agentů, případně digitální peněženek, je tato varianta nejsnazší, nicméně v průběhu implementace nemáte úplnou kontrolu nad daným prostředím.

Testovací prostředí nemají garantovanou dostupnost a během implementace byly občas neresponzivní, zejména v případě ověřování vlastních záznamů na blockchainu. Další možností je vytvoření vlastního testnetu, kdy máte plnou kontrolu nad blockchainem.

Pro spuštění vlastního testnetu bylo využito řešení tzv. VON networku [50], který je implementací Hyperledger Indy poskytovanou pro kanadský region Britské Kolumbie. Součástí této implementace je nejen blockchain ale i webová prohlížečka záznamů na blockchainu. Bez webového prohlížečky je pro prohlížení na blockchainu nutné použít CLI (command line interface) Indy a poté se připojit na specifický nod. Uvedené řešení je poskytované s volně šiřitelnou licencí Apache 2.0. Při využití této implementace pomocí docker images není nutné řešit problémy spojené s interoperabilitou Indy s operačním systémem, jelikož Indy v případě vlastní kompilace vyžaduje pouze Ubuntu 18.

5.2.1 Infrastruktura

Prerekvizitou pro spuštění vlastního testnetu je vystavení aplikace do internetu, tak aby jednotlivé nody běžely na veřejné IP adrese. Kompletní implementace řešení byla vzhledem k dané prerekvizitě vytvořena v AWS. Vzhledem k tomu, že se jedná o ukázkové řešení byla vytvořena EC2 instance (ekvivalent virtuálního serveru) s veřejnou IP adresou. Jednotlivé blockchainové nody na dané EC2 instanci byly vystaveny na portech 9701-9708. Otevření těchto portů do internetu bylo provedeno prostřednictvím tzv. „security groups“ pro všechen provoz na TCP protokolu pro dané porty.

Základní konfigurace testnetu spočívá v definování veřejné IP adresy nodů, portů a seedu pro generování genesis souboru. Soubor je poté mandatorní pro prvotní připojení jakýchkoliv agentů k blockchainové síti, poukazuje, na jakých IP adresách je decentralizovaná síť dostupná.

V rámci Hyperledger Indy genesis soubor obsahuje důležité informace nutné pro agenty, kteří se budou chtít k síti připojit. Genesis soubor obsahuje informací o:

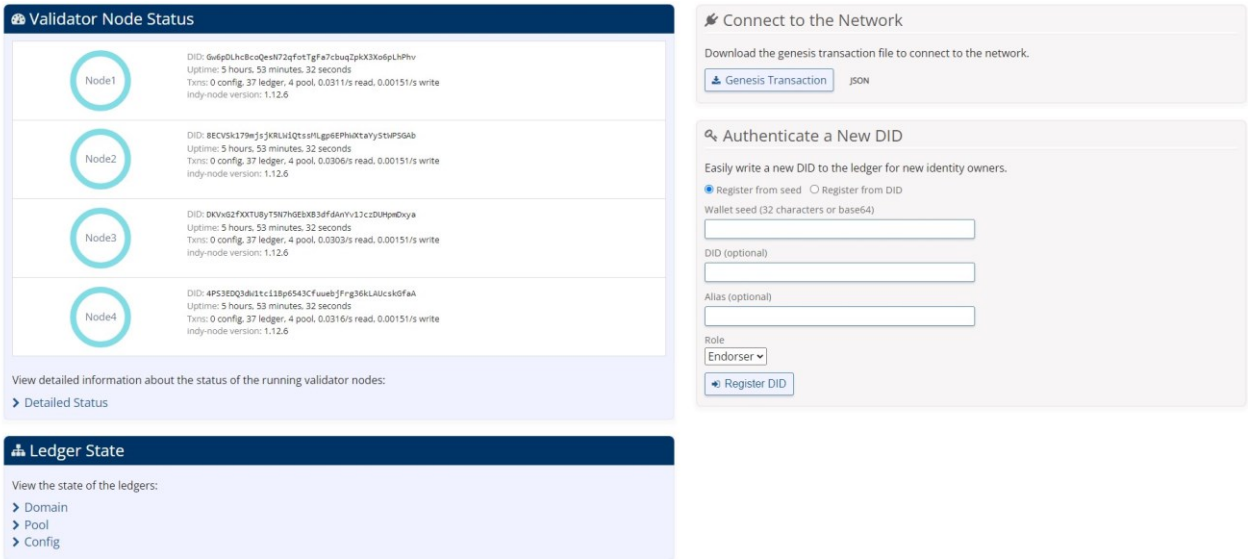
- IP adresách a portech o prvotních nodech z ledger poolu (tyto informace jsou uloženy po startu na ledger a pokud se přidají nové nody do sítě, je jejich záznam přidán na ledger)
- Veřejné klíče nodů
- Informace pro připojení i pro agenty/digitální peněženky
- Genesis file má informací o prvních transakcích na ledgeru, tzv. genesis blok

```
{"reqSignature":{},"txn":{"data":{"data":{"alias":"Node1","blskey":"4N8aUNHSgjQVg-
kpm8nhNEfDf6txHznoYREg9kirmJrkivgL4oSEimFF6nsQ6M41QvhM2Z33nves5vfSn9n1UwNFJBYtWVnHY-
MATn76vLuL3zU88KyeAYcHfsih3He6UHcXDxcaecHVz6jhCYz1P2UZn2bDVruL5wXpehg-
BfBaLKm3Ba","blskey_pop":"RahHYiCvoNCtPTrVtP7nMC5eTYrsUA8WjXbdhNc8debh1agE9bGiJxWBXYNFbn-
JXoXhWFMvyqhqhRoq737YQemH5ik9oL7R4NTTCz2LEZhkgLJzB3QRQqJyBNyv7acbdHrAT8nQ9UkL-
baVL9NBpnWXBTw4LEMePaSHEw66RzPN-
dAX1","client_ip":"16.16.241.83","client_port":9702,"node_ip":"16.16.241.83","node_port":97
01,"servi-
ces":["VALIDATOR"]},"dest":"Gw6pDLhcBcoQesN72qfotTgFa7cbuqZpkX3Xo6pLhPhv"},"metadata":{"fro
m":"Th7MpTaRZVRYnPiabds81Y"},"type":"0"},"txnMeta-
data":{"seqNo":1,"txnId":"fea82e10e894419fe2bea7d96296a6d46f50f93f9eeda954ec461b2ed2950b62"
},"ver":"1"}
```


Obrázek 18. Část genesis file v json formátu [66]

5.2.2 Hyperledger Indy web

Webová prohlížečka poskytuje náhled na jednotlivé záznamy uložené na blockchainu,ak ktuální stav připojených nodů, možnost si stáhnout genesis soubor a případně ručně zavést nový DID s definovanými právy na blockchainu. Role v rámci Hyperledger Indy budeme řešit v rámci diskuze produkčního řešení Hyperledger Indy.



Obrázek 19. Web náhledu na Indy blockchain [66]

5.2.3 Produkční systém

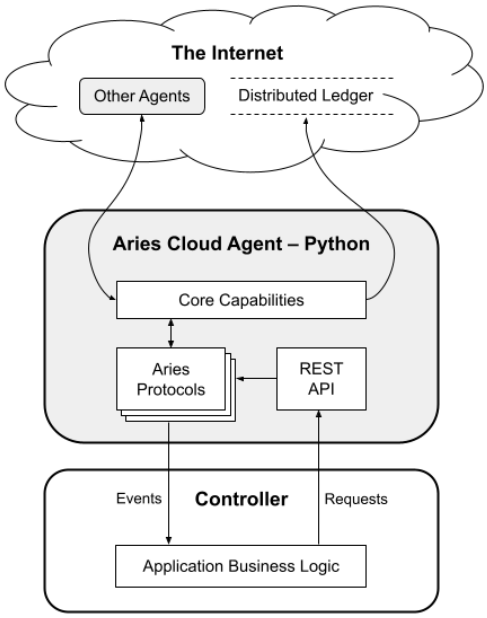
Pro eventuální vystavení blockchainu do produkčního prostředí je nutné řešit několik bodů před samotným nasazením.

- Definice procesů (v našem ukázkovém případě nejsou řešeny procesy potvrzování a validování transakcí, transakce jsou schvalovány automaticky, nicméně v produkčním prostředí jsou správně nastavené procesy nutnost)
- Vydefinovat role a práva jednotlivých účastníků (existují role Trustee, Steward, Endorser, Network Monitor) [52]
- Vydefinovat podmínky použití, tzv. Transaction Author Agreement (TAA). Jedná se o akceptování podmínek použití služeb, především v případě zapisování dat na blockchain. TAA je možné přirovnat k akceptování End User Agreement (EULA), když chceme využívat něčí služby. [51]
- Je nutné brát v potaz další legislativní překážky jako GDPR. Ideální příklad je právo na výmaz, kdy transakce na blockchainu jsou uloženy permanentně bez možnosti odstranění. Taková data je tedy nutné ukládat a spravovat mimo blockchain.
- Zabezpečení vlastní infrastruktury provozovaného nodu

5.3 Agent pro komunikaci s VDR

Pro komunikaci s blockchainem byl v práci využit framework Hyperledger Aries, který poskytuje knihovny a nástroje pro práci s digitální identitou. Obecně není vázaný na žádný blockchain, jedná se o tzv. blockchain agnostic systém, nicméně jako první byla vytvořena implementace pro komunikaci s Hyperledger Indy. Samotný Hyperledger Aries využívá komponenty dalších produktů Hyperledgeru.

Agent zprostředkovává komunikaci s blockchainem a ostatními agenty, viz. obrázek 19. Dále interaguje ještě s controllerem, který je v našem případě webový server.



Obrázek 20. Role Hyperledger Aries [53]

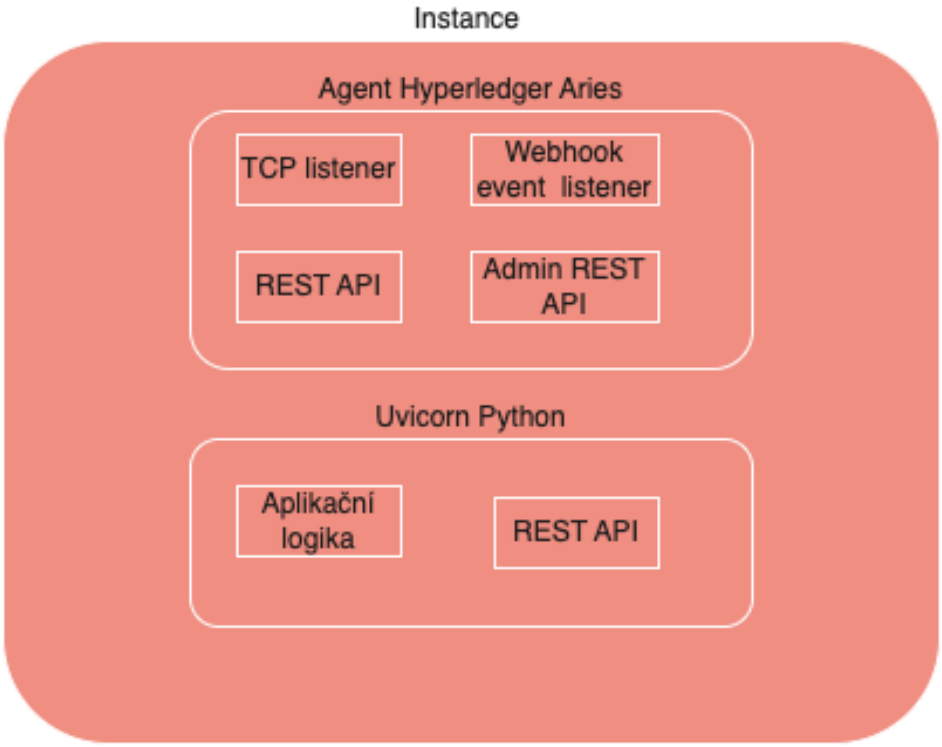
5.4 Backend který komunikuje s VDR

Implementace backendů z pohledu jednotlivých komponent byla navržena téměř totožně pro roli issuera i verifiera. Z pohledu využití v produkčním prostředí budou v následujících kapitolách diskutovány důležité poznámky, které bude v takovém případě brát na vědomí.

Instance obsahuje dvě základní komponenty:

- Uvicorn (implementace web serveru pro python)
- Agent Hyperledger Aries

Kdy implementace Python webserveru má vystaveno REST API pro frontendovou aplikaci, díky které interaguje s agentem. Tento agent poté komunikuje s blockchainem a jinými agenty.



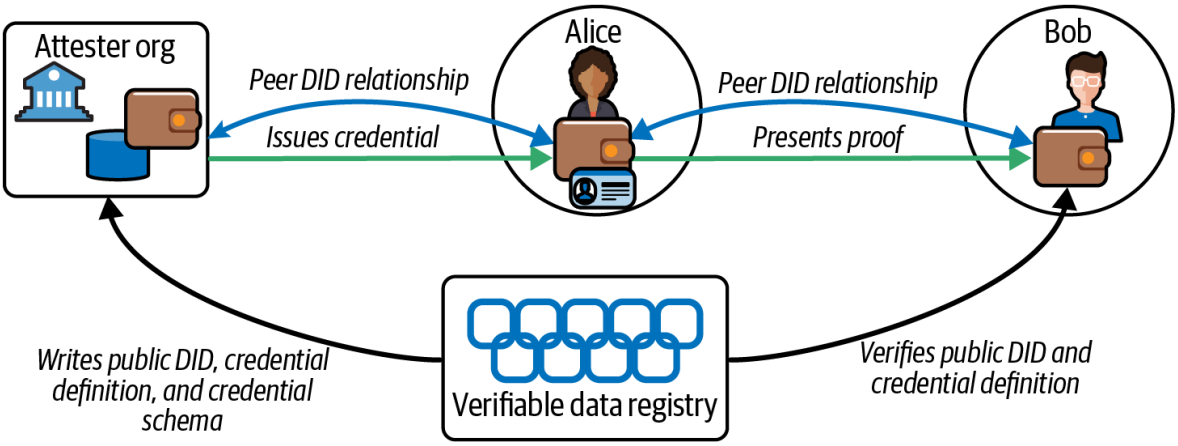
Obrázek 21. Komponenty instance backendu [66]

5.5 Definice rolí a identity

V kapitole 6 byl již definován high level scénář, který specifikoval typ identit, které bude nutné navrhnout. Tato kapitola popíše chování těchto účastníků a bude diskutovat řešení.

Ukázková implementace obsahuje dva typy identity, a to konkrétně identitu osoby (ekvivalent atributů popisovaných v občanském průkazu) a poté identitu v rámci komunity (ekvivalent zaměstnaneckých přístupů do sdílené sítě korporátu, přístupu odborných fór, služby využívající univerzitních přístupů a mnoho dalších).

Definujme ji tedy jako ekvivalent občanského průkazu, která je vydána důvěryhodným vydavatelem identity, tento vydavatel identity bude v případě této implementace definován jako „**Issuer**“. Dále definujme identitu vydávanou v rámci komunitní sítě, tato identita je vydána pouze pod podmínkou, že uživatel je schopný se prokázat svojí vlastní identitou a tím pádem prokázat, že se jedná o reálnou osobu. Zároveň je vyžadováno poskytnutí potvrzení, že je zákazník starší více než 18let, a to pomocí ZKP.



Obrázek 22. Jednoduchá implementace SSI s jedním dokladem [26]

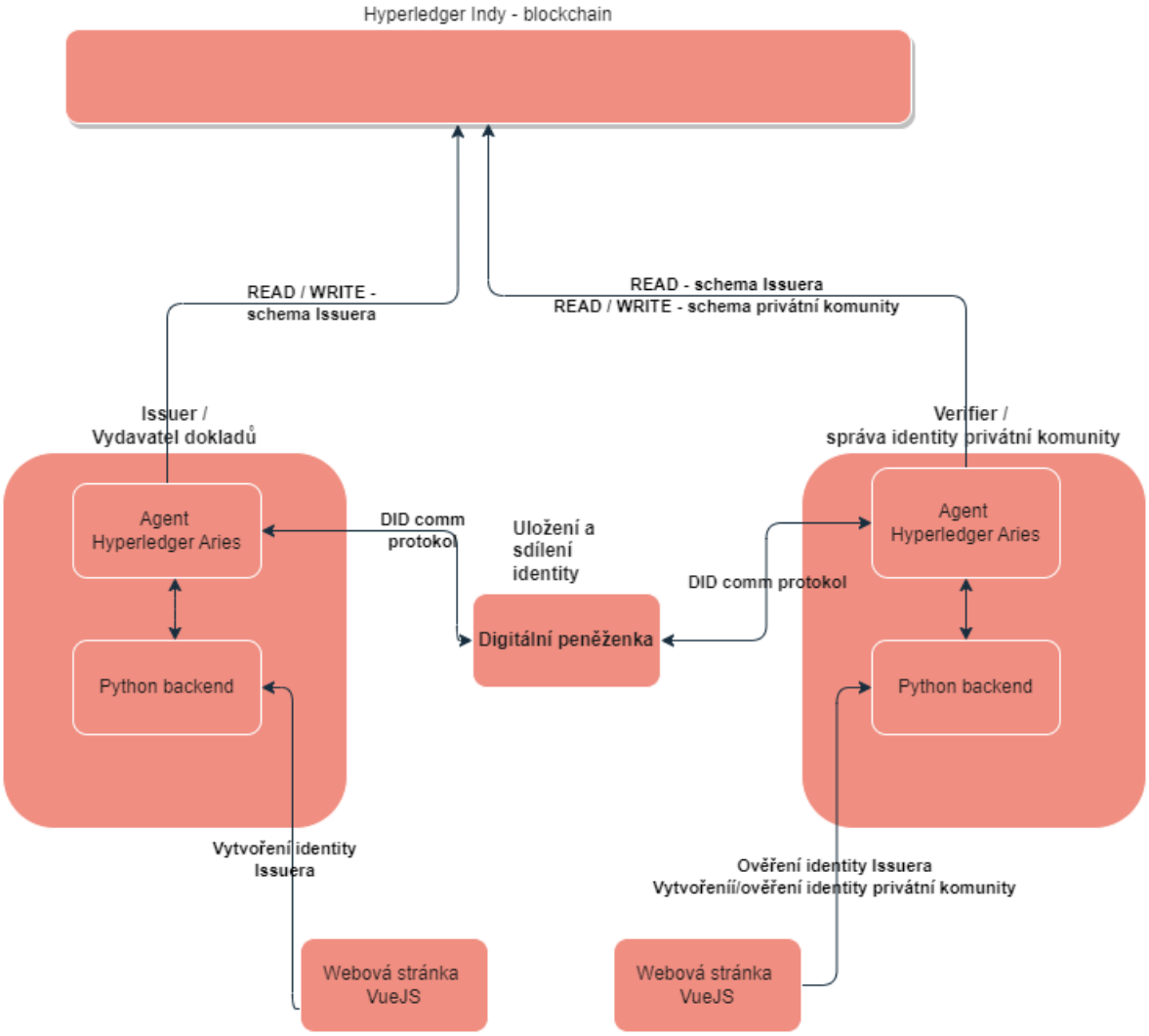
V rámci implementace definujeme vlastnosti agenta a funkce nezbytné pro definici systému:

5.5.1 Agent Issuer

Issuer je dle definovaných vlastností na obr. 21 možný zapisovat ale i číst z blockchainu. Především se jedná o zápis veřejného DID, schémata a credentials definition dokladu. V reálném prostředí by se jednalo o definici a schéma struktury oficiálního vydávaného dokumentu. V ukázkové implementaci byla využita definice osoby dle schématu osoby veřejně dostupné na https://schema.org/Person. Tuto identitu poté mohou odeslat do digitální peněženky.

5.5.2 Agent Verifier

Verifier je agent, který je součástí řešení modelového webu. Svými vlastnostmi musí být schopen číst z blockchainu a zároveň musí být schopný vytvářet schéma a credentials definition pro privátní komunitu. Zároveň také komunikuje s digitální peněženkou (tzv. Holderem).



Obrázek 23. Schéma jednotlivých komponent řešení [66]

5.5.3 Digitální peněženka

V rámci diplomové práce využijeme digitální peněženky třetích stran, které jsou interoperabilní s naším řešením. Hyperledger Aries aktuálně definuje dvě verze AIP1.0 a AIP 2.0 (Aries Interop Profile), což je sada vydefinovaných vlastností, které musí agenti splňovat, tak aby byly interoperabilní mezi sebou. Bohužel žádná z testovaných peněženek nepodporuje AIP 2.0., který nabízí novější formáty DID a VC. Všechny testované peněženky podporují AIP 1.0. [54]

5.6 Poskytovatel digitální peněženky

Jako poskytoval digitální peněženky je třeba řešit nejen mobilní aplikace nejen z pohledu interoperability, bezpečnosti, ale především i z pohledu legislativního rámce. V případě rozšířené aplikační logiky je možné poskytovat, tzv. mediační služby. Kdy poskytovatel nabízí rozšířenou aplikační logiku nad digitální peněženkou. Například zálohování dat na externích uložištích, push notifikace etc.

6 APLIKACE

6.1 Start aplikace

Start aplikace probíhá následovně v případě Issuera i Verifiera (pouze se liší porty aplikací):

- Nastartování webserveru (uvicorn) na portu 8000 pro issuera (8100 pro verifiera)
- Webserver nastartuje asynchronní proces pro spuštění agenta
- Při iniciliaziaci objektu Issuera či Verifiera dochází ke spuštění instance Aries agenta
- Aries agent beží na portech 8020, 8021 a 8022 pro issuera (8030-8032 pro verifiera)
- Na portu 8020/8030 TCP běží listener pro komunikaci s ostatními agenty (tzv. DID-comm protokol viz. kapitola 2.8.5)
- Na portu 8021/8031 běží admin API pro operace s agentem
- Na portu 8022/8032 poslouchá webhook, který zpracovává příchozí události
- Agent si stáhne aktuální nastavení genesis souboru z důvodu načtení informací nutných pro připojení (IP adresy, veřejné klíče)
- Agent zaregistruje svůj veřejný DID a v případě této implementace je mu nastavena i schopnost potvrzovat transakce, tzv. role „Endorser“
- Agent získal veřejný DID, může tedy registrovat schéma a credentials definition verifiable credentials na blockchain
- Schéma registrace probíhá je inicializováno POST požadavkem na blockchainovou instanci

Obrázek 24. Požadavek na založení schématu [66]

Obrázek 25. Schéma uloženo na blockchainu [66]

- Po zaregistrování schématu je registrováno schema definition s vazbou na veřejný DID agenta

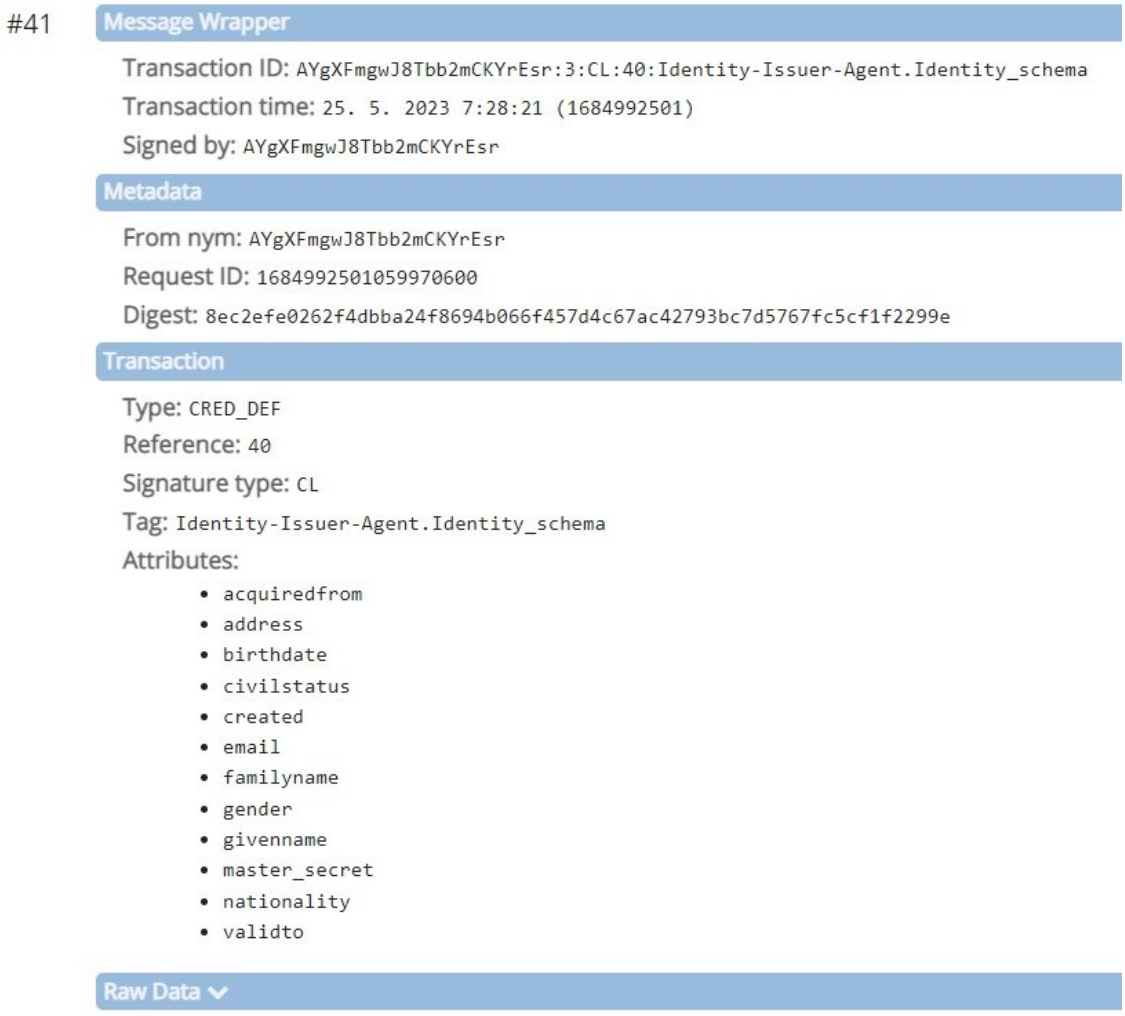
```
Schema ID: AYgXFmgwJ8Tbb2mCKYrEsr:2:Identity schema:67.70.10

EVENT: Controller POST /credential-definitions request to Agent with data:
{
    "schema_id": "AYgXFmgwJ8Tbb2mCKYrEsr:2:Identity schema:67.70.10",
    "support_revocation": false,
    "tag": "Identity-Issuer-Agent.Identity_schema"
}

EVENT: Response from POST /credential-definitions received:
{
    "sent": {
        "credential_definition_id": "AYgXFmgwJ8Tbb2mCKYrEsr:3:CL:40:Identity-Issuer-Agent.Identity_schema"
    },
    "credential_definition_id": "AYgXFmgwJ8Tbb2mCKYrEsr:3:CL:40:Identity-Issuer-Agent.Identity_schema"
}
```

Obrázek 26. Požadavek na založení credentials definition

- V rámci záznamů na blockchainu jsou uloženy informaci o schématu verifiable credentials na blockchainu a především hashe daných atributů schématu



Obrázek 27. Credentials definition zapsané na blockchainu [66]

Identický proces probíhá jak na straně agenta Issuera (schéma VC pro Identitu) tak Verifiera (schéma VC pro „komunitní identitu“)

Z pohledu agenta v uvedeném scénáři žádné další operace se zápisem na blockchain nebudeme provádět. Další operace budou sloužit k vytváření VC a ověřování VC na základě uložených dat na blockchainu. Nicméně v produkčním prostředí se nabízí implementace rolí zmíněných v kapitole 6.2.3, kdy by samotný agent neměl práva na schválení zapsání daného schématu na blockchain a musel by požádat jiného agenta s dostatečnými právy.

Spuštění aplikací obou agentů je možné pomocí dockerfilu, které jsou součástí kódu. Je to doporučený způsob z důvodu interoperability na různých operačních systémech. Především používané Hyperledger Indy knihovny v rámci frameworku Hyperledger Aries jsou nutné

pro komunikaci s blockchainem a mají limitaci na Python 3.6–3.7. V rámci dockerfilu je nutné definovat ip adresu a port digital ledger. Vystavení DLT na doménu byla testována, nicméně komunikace mezi nody blockchainu nebyla úspěšná. Co se týče agenta, tak je možné jej vystavit bez problémů na doménu. Komunikace mezi agenty probíhá přes internet.

```
ENV LEDGER_URL "http://${IP_ADRESA}:${PORT}"
ENV AGENT_ENDPOINT "http://${IP_ADRESA}:${PORT}""
```

6.2 Komunikace s ostatními agenty

Komunikace s ostatními agenty je prostřednictvím takzvaného DIDcomm protokolu. Jedná se o TCP/IP protokol. Komunikace tedy začíná otevřením socketu na dříve uvedených portech 8020 a 8030. Při navázání komunikace probíhá tzv. výměna DID, kdy dva agenti navážou konektivitu a uloží si veřejné klíče spolu s DID identifikátorem. Agenti běžící na serveru (v našem případě Issuer a Verifier) tedy musí tyto informace bezpečně uložit a to do tzv. serverové peněženky. Hyperledger Aries podporuje použití více typů serverových peněžek, nicméně v práci je využit nativní formát Hyperledger Askar. Tento formát peněženky je možné držet na disku či v databázi. V rámci práce je použito defaultní nastavení, kdy dojde při každé inicializaci agenta k vytvoření nové serverové peněženky.

Agenti můžou tedy navazovat spojení jak mezi sebou z pohledu serverů, tak i s mobilními digitálními peněženkami. Musí také v rámci interoperability komunikovat pomocí DIDcomm protokolu a pracovat s DID dokumenty, takže je možné konstatovat, že jsou také agenti. Jak již bylo řečeno mobilní digitální peněženky i agenti budovat kompatibilní s tzv. AIP v 1.0.

6.3 Webová aplikace

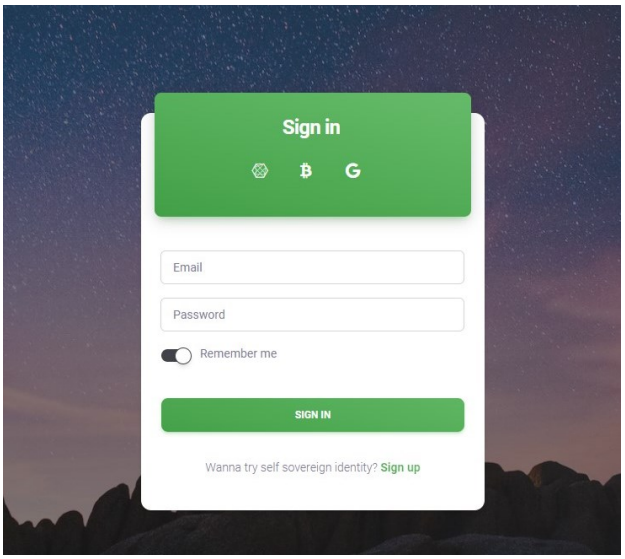
Hlavním cílem webové aplikace je poukázat na možnou aplikovatelnost přihlašování pomocí decentralizované identity v reálném řešení. Uživatel je potencionální uživatelem služeb komunity, která svými podmínkami limituje možnost využití služeb všem zákazníkům mladších osmnácti let. Uživatel při přechodu na webovou stránku nevlastní vůbec žádnou identitu, pouze vlastní prázdnou mobilní digitální peněženku. Bude tedy popsán i proces získání své digitální identity, která by prokazovala jeho věk. A na základě této identity mu bude poskytnuta možnost vytvoření identity v rámci komunitních služeb.

Z technického pohledu se jedná o standardní frontendovou aplikaci založenou na frameworku Vue3 s využitím komponent „MaterialKit“. Aplikace je tedy napsána v javascriptu,

HTML a CSS. Pro snadné nasazení aplikace je v přiložených kódech Dockerfile, který v první kroku provede build aplikace a následný výstup je nakopírován do image, která vychází z nginx. Aplikace je vystavena dle repozitáře nastavena na portu 8029, nicméně toto chování je pouze pro snížení rizika útoků na aplikaci během testů z důvodu testování v internetu. V produkčním řešení by aplikace běžela na standardním portu 443 pro HTTPS a web server by byl zabezpečený buď tzv. „web application firewallem“ nebo alespoň pravidly mod security.

6.3.1 Vstupní stránka webu

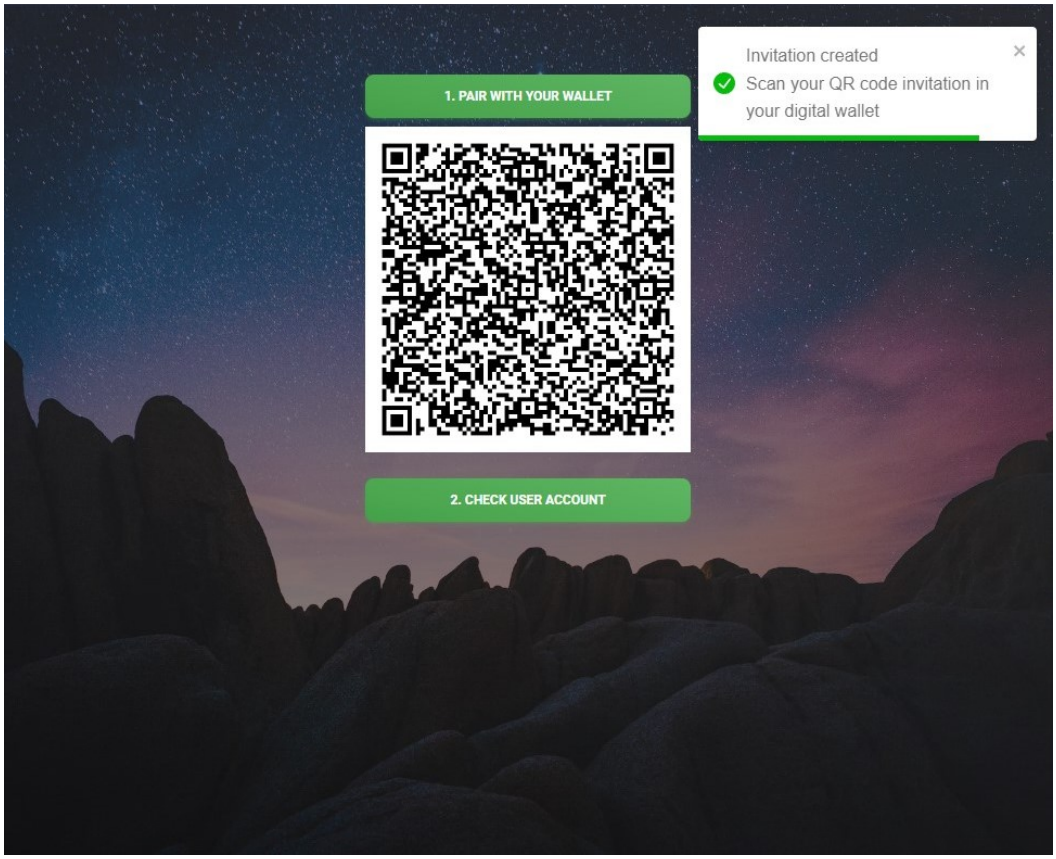
Přihlášení uživatele standardně využívá centralizovaného identity systému (tzn. přihlašování jménem a heslem), kdy veškeré údaje jsou ve vlastnictví provozovatele webu. Další možností je využití federovaných identity služeb např. Googlu, kdy ověření identity probíhá na serverech provozovatele federované identity, který je zároveň vlastníkem těchto údajů. Další možností je přihlášení pomocí SSI.



Obrázek 28. Landing page [66]

6.3.2 Propojení s agentem komunity

Uživatel se po prokliku dostane na web agenta, který je v ukázkovém případě součástí webu privátní komunity. Pro vytvoření spojení mezi agentem a digitální peněženkou je nutné naskenovat uvedený QR kód. Na pozadí peněženka provede navázání spojení a výměnu DID. Skenování QR kódu je všeobecně uznávaný proces ve všech digitálních mobilních peněženkách pro identitu.



Obrázek 29. Navázání spojení [66]

V prvním kroku je třeba navázat komunikaci mezi agentem webové aplikace a digitální peněženkou. QR code obsahuje odkaz pro kontaktování agenta komunity (Verifier) pro navázání kontaktu. Po navázání spojení je možné dále mezi sebou interagovat. Pro popis řešení využijeme digitální peněženku „Trinsic Wallet“ z důvodu kompatibility s AIP 1.0. a podpory privátních blockchainových sítí (vlastního testnetu).

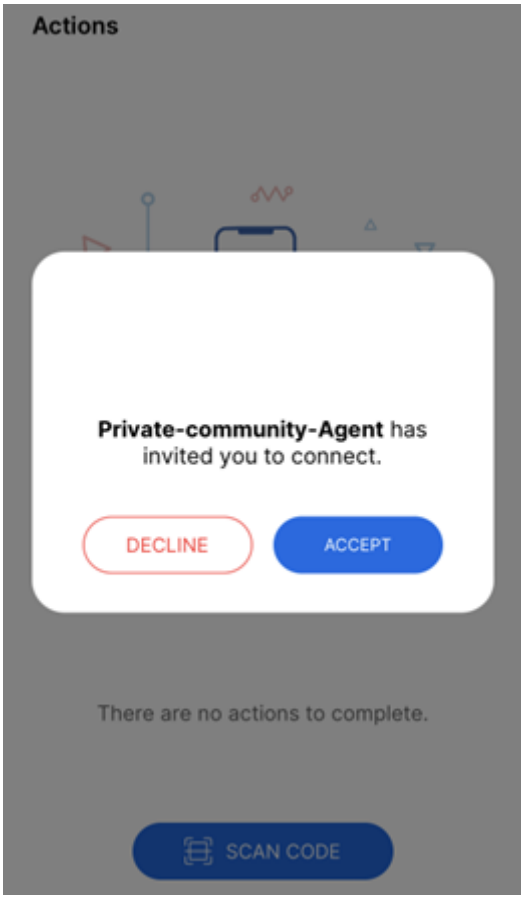
```
EVENT: Agent called controller muj novy webhook: handle_connections
POST http://localhost:8032/webhooks/topic/connections/ with payload:
{
    "invitation_mode": "once",
    "their_role": "invitee",
    "state": "request",
    "rfc23_state": "request-received",
    "their_did": "BLU7pKrwrtYnaJgzBFgaiT",
    "routing_state": "none",
    "connection_id": "a0856899-f715-4f21-8df9-7cfe8155c3a0",
    "updated_at": "2023-05-25T07:30:10.610270Z",
    "connection_protocol": "connections/1.0",
    "created_at": "2023-05-25T07:29:47.222851Z",
    "their_label": "iPhone",
    "accept": "auto",
    "invitation_key": "EeLE8NfYMRJHjxB4beKVJspiyZtwt2r3sM7f4i4Dh69z"
}


EVENT: Agent called controller muj novy webhook: handle_connections
POST http://localhost:8032/webhooks/topic/connections/ with payload:
{
    "invitation_mode": "once",
    "their_role": "invitee",
    "state": "response",
    "rfc23_state": "response-sent",
    "their_did": "BLU7pKrwrtYnaJgzBFgaiT",
    "routing_state": "none",
    "connection_id": "a0856899-f715-4f21-8df9-7cfe8155c3a0",
    "updated_at": "2023-05-25T07:30:10.642717Z",
    "my_did": "hQa59hMPvF97jCGbooo5U",
    "connection_protocol": "connections/1.0",
    "created_at": "2023-05-25T07:29:47.222851Z",
    "their_label": "iPhone",
    "accept": "auto",
    "invitation_key": "EeLE8NfYMRJHjxB4beKVJspiyZtwt2r3sM7f4i4Dh69z"
}
```


Obrázek 30. Navázání spojení z pohledu serverového agenta

Dle logů na obrázku 29 je možné pozorovat výměnu DID dokumentů mezi serverovým agentem a digitální peněženkou. Na obrázku 30 poté navázání spojení z pohledu mobilní peněženky.

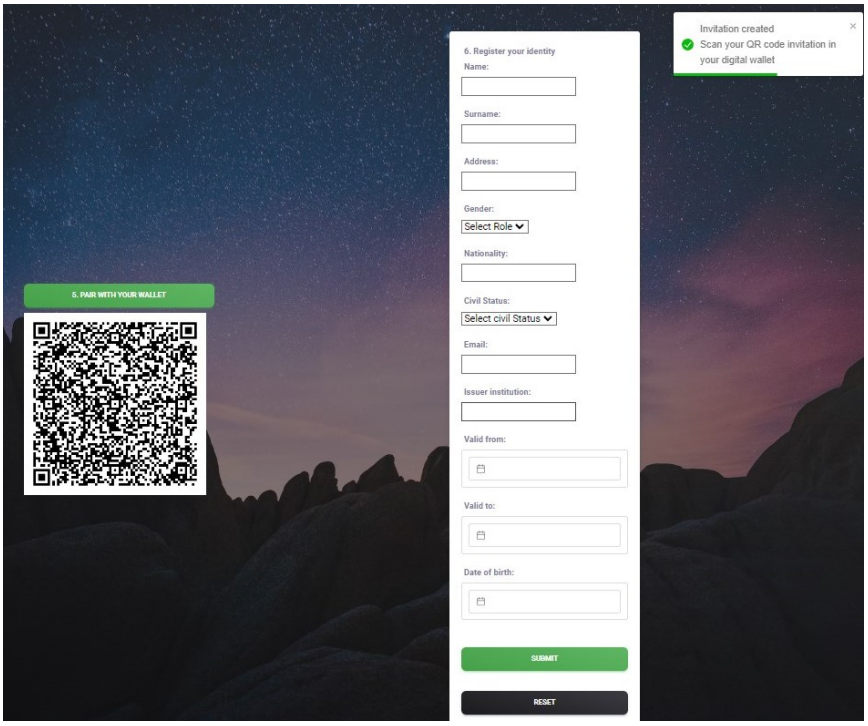
Uživatel může oproti blockchainu možnost ověřit identitu zákazníka, případně jestli již vlastní účet. Nicméně VC v daném kroku ještě nevlastní.



Obrázek 31. Navázání spojení z pohledu mobilní peněženky

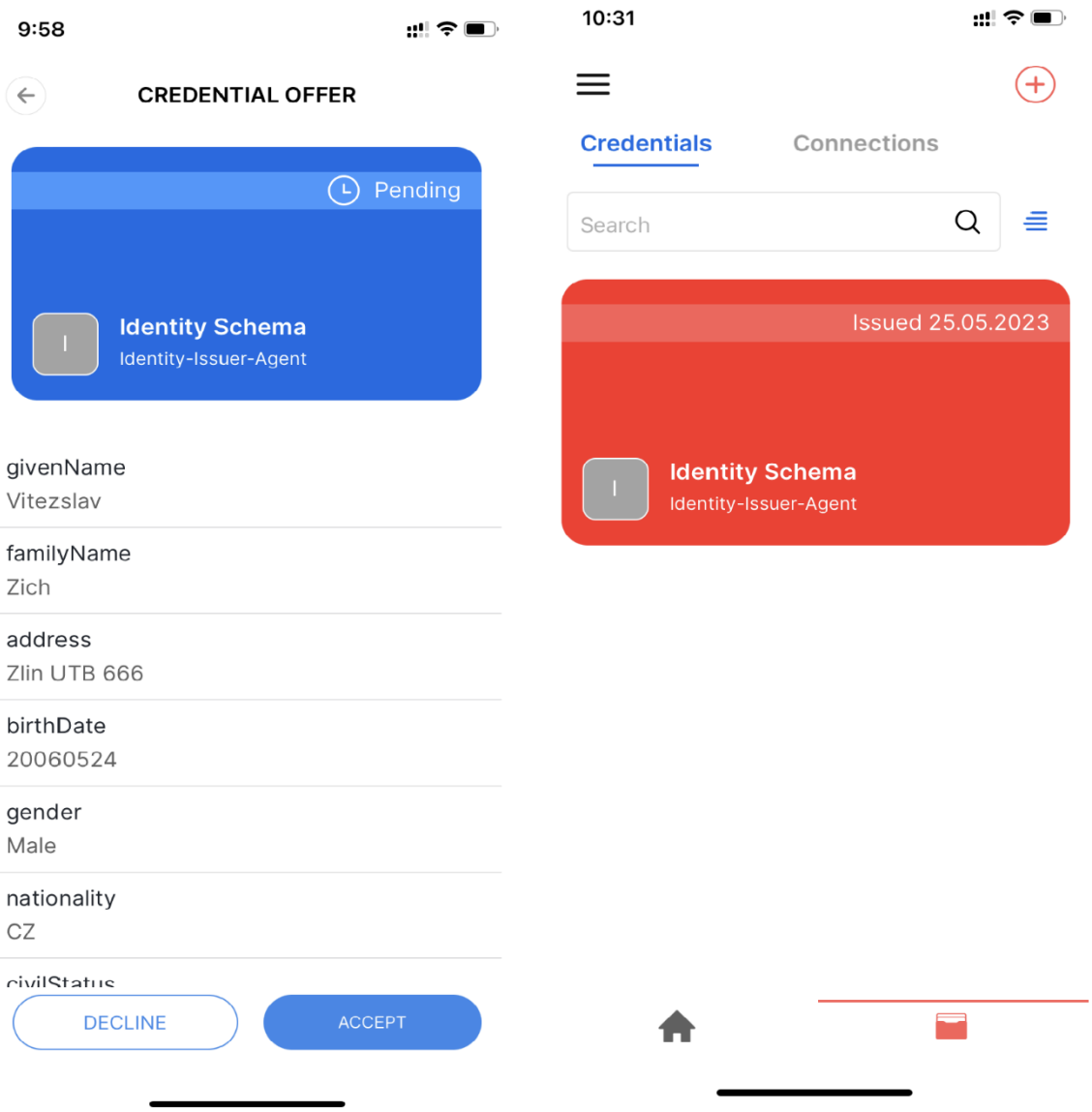
6.3.3 Propojení a vydání identity na straně issuera

V uvedeném řešení je uživatel přesměrován na web issuera, který vydává identitu jako takovou. V reálném scénáři se jedná o poskytovatele digitální identity (např. web státní správy s formulářem o žádost vydání digitální identity). Jedná se tedy z pohledu funkcionality o jiný web, tzn. nová instance agenta. Je nutné navázat spojení i s touto entitou. Po navázání spojení můžeme vytvořit požadavek na vydání VC, tzv. „credentials request“. V ukázkovém řešení dojde automaticky ke schválení požadavku na vydání VC, nicméně v reálné situaci by musel uživatel s žádostí pravděpodobně na nejbližší pobočku státní správy, případně využít jiný kanál (i online), kterým by dokázal prokázat sám sebe.



Obrázek 32. Webová stránka Issuera [66]

V mobilní peněžence obdržíte push notifikaci, že Vám v rámci spojení byl nabídnut VC. Po akceptování dojde ke komunikaci mezi agenty a VC můžete poté využívat. V digitální peněžence nicméně musíte být připojení k blockchainu (VDR) pro kterou serverový agent VC vydal. Uvedené řešení neukládá žádné údaje na blockchain ohledně vydané identity. Agenti validují, zda credentials schema a definition odpovídají vydanému dokladu.



Obrázek 33. Nabídka a uložení dokladu v peněžence [66]

6.3.4 Vytvoření identity komunity

Doklad vydaný v předchozím kroku, nyní můžete využít pro ověření své identity. Možnost ověřit uvedený doklad může i agent soukromé komunity. Credentials schema a definition jsou totiž uloženy na blockchainu. V reálném prostředí bude největší omezení fakt, zda ověřovatel dostatečně důvěřuje vydavateli dokladu.

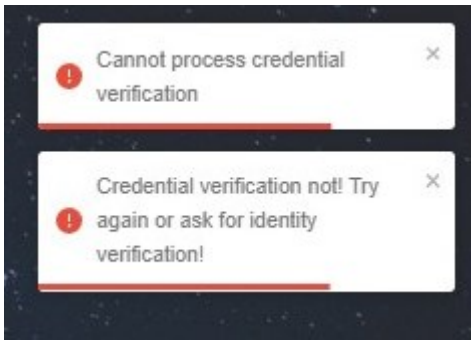
```
                {
                    "schema_name": "Identity schema"
                }
            ],
            "name": "givenName"
        },
        "0_familyName_uuid": {
            "restrictions": [
                {
                    "schema_name": "Identity schema"
                }
            ],
            "name": "familyName"
        },
        "0_email_uuid": {
            "restrictions": [
                {
                    "schema_name": "Identity schema"
                }
            ],
            "name": "email"
        },
        "0_validTo_uuid": {
            "restrictions": [
                {
                    "schema_name": "Identity schema"
                }
            ],
            "name": "validTo"
        },
        "0_address_uuid": {
            "restrictions": [
                {
                    "schema_name": "Identity schema"
                }
            ],
            "name": "address"
        }
    },
    "requested_predicates": {
        "0_birthDate_GE_uuid": {
            "name": "birthDate",
            "restrictions": [
                {
                    "schema_name": "Identity schema"
                }
            ],
            "p_value": 20050525,
            "p_type": "<="
        }
    }
},
"verified": "true",
"auto_present": false,
"connection_id": "9742742d-4f05-4a62-8f49-4d392ada7ee0",
"thread_id": "a5762706-76ce-4154-ace0-d8740bb4f7ee",
"presentation_exchange_id": "a2537305-0ee7-4b15-9c0b-bd5e0c14ba31",
"initiator": "self",
"trace": false
```


Obrázek 34. Selective disclosure [66]

Na obrázku 33 je záznam komunikace mezi peněženkou a serverovým agentem, informace týkající se splněné podmínky věku není uvedena v logu a nedochází k jejímu zaslání. Je pouze ověřena pomocí ZKP pro Hyperledger Indy. Na základě ověření můžete požádat o vydání nového dokladu.

6.3.5 Test věku pomocí selective disclosure

V rámci řešení proběhl také test nedostatečného věku v digitální peněžence. V peněžence byla vydána identita s věkem pod 18 let. V tomto případě nebyla daný uživatel nevlastnil danou idenitu a byla tedy zamítnuty viz. obrázek 34.



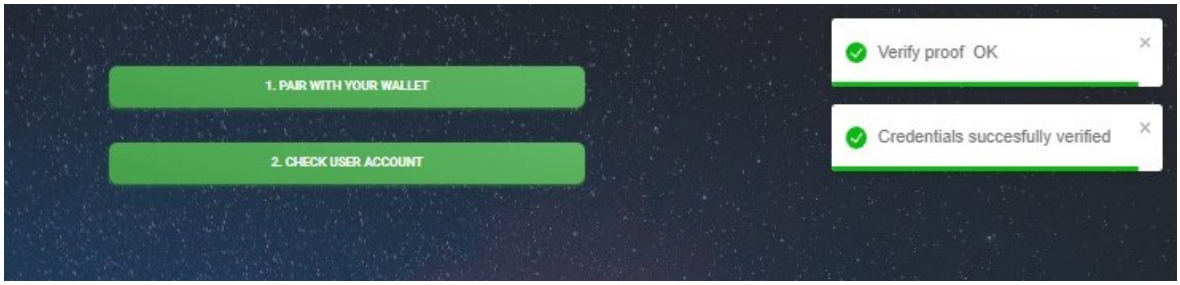
Obrázek 35. Test věku [66]

```
req_preds = [
    # test zero-knowledge proofs
    {
        "name": "birthDate",
        "p_type": "<=",
        "p_value": int(birth_date.strftime(birth_date_format)),
        "restrictions": [{"schema_name": schema_name}],
    }
]
indy_proof_request = {
    "name": "Proof of Identity",
    "version": "1.0.0",
    "requested_attributes": {
        f"0_{req_attr['name']}_uuid": req_attr for req_attr in req_attrs
    },
    "requested_predicates": {
        f"0_{req_pred['name']}_GE_uuid": req_pred for req_pred in req_preds
    },
}
```

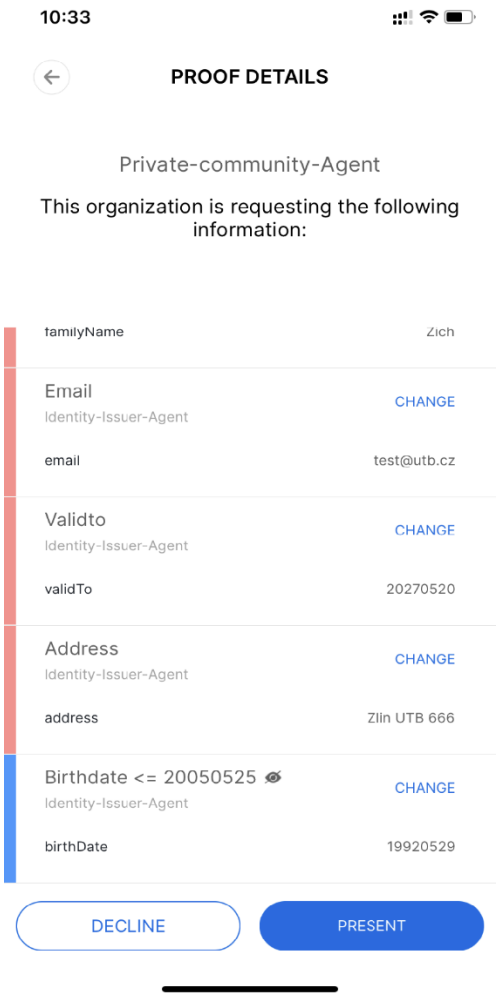
Obrázek 36. Implementace ověření věku [66]

6.3.6 Ověření identity komunity

S vydáním dokladu komunity přichází poslední krok uvedeného flow a to ověření uvedeného dokladu. Principiálně je proveden stejný proces jako v případě ověření identity vydané issuerem. Po úspěšném ověření už je možné přidat další aplikační logiku. Jako uložení sdílených údajů do databáze přihlášených účtů v rámci služby, kterou chtěl uživatel použít. Získání např. session ID a přesměrování na požadované služby komunity.



Obrázek 37. Finální ověření z pohledu webu [66]



Obrázek 38. Požadavek na ověření z pohledu peněženky [66]

6.4 Testy digitálních peněženek

V rámci praktické části bylo testováno implementované řešení s několika komerčními digitálními peněženkami. Všechny peněženky splňovali kompatibilitu s verzí protokolu AIP 1.0, který zahrnuje doporučené implementace agenta dle tzv. „Request for comments“ (RFC). Aktuálně existují dvě verze protokolu AIP v 1.0 a AIP v 2.0. Verze 2.0. je nicméně ještě v procesu standardizace, kdy neobsahuje všechny očekávané vlastnosti pro možnou plnou funkčnost agenta. Z pohledu digitálních peněženek pro uživatele mobilních aplikací jsou momentálně podporovány pouze peněženky s verzí AIP 1.0. Z tohoto důvodu proběhlo testování a ověření vlastní implementaci na těchto peněženkách. [55]

6.4.1 Trinsic Wallet

Digitální peněženka Trinsic Wallet je distribuována na obou mobilních platformách iOS i Android. Nicméně v případě Androidu je aplikace již zastaralá pro nejnovější Android verze. Firma Trinsic se obecně zabývá obecně identitou a prodává na svém webu i ostatní identity služby.[56]

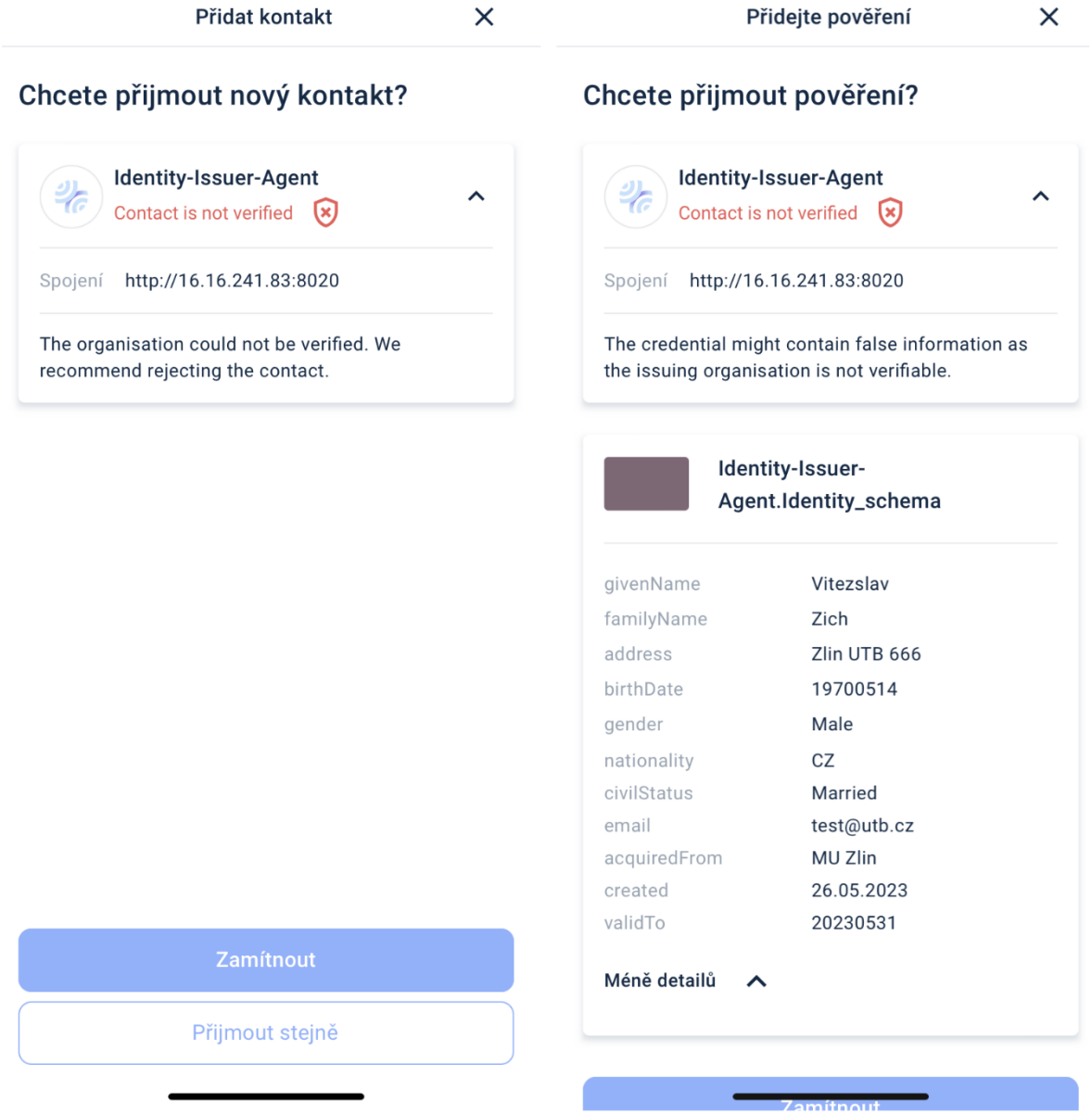
Mobilní peněženka byla testována v rámci celého implementovaného řešení, viz. předchozí screenshoty. Podporovala propojení s agenty Issuera i Verifiera. Přidání privátní blockchainové sítě v případě ukázkové implementace soukromého testnetu. Umožňovala uložit i ověřit vydané doklady.

Nevýhody aplikace jsou zastaralá podpora OS Android.

6.4.2 Lissi Wallet

Digitální peněženka Lissi Wallet je nabízena jako jediný produkt. Aktuálně probíhá na jejich straně implementace agentů pro decentralizovanou identitu. Mobilní aplikace je distribuována jak na iOS, tak i Android. [57]

Mobilní peněženka byla testována ve stejných podmínkách jako předchozí Trinsic wallet. Lissi podporuje jak navázání spojení, tak i přidání vlastního blockchainu. Uložení a ověření dokladů proběhlo korektně, viz. obrázek 38. Aplikace zároveň varovala na naše agenty, protože nebyly vedeni jako ověření agenti.

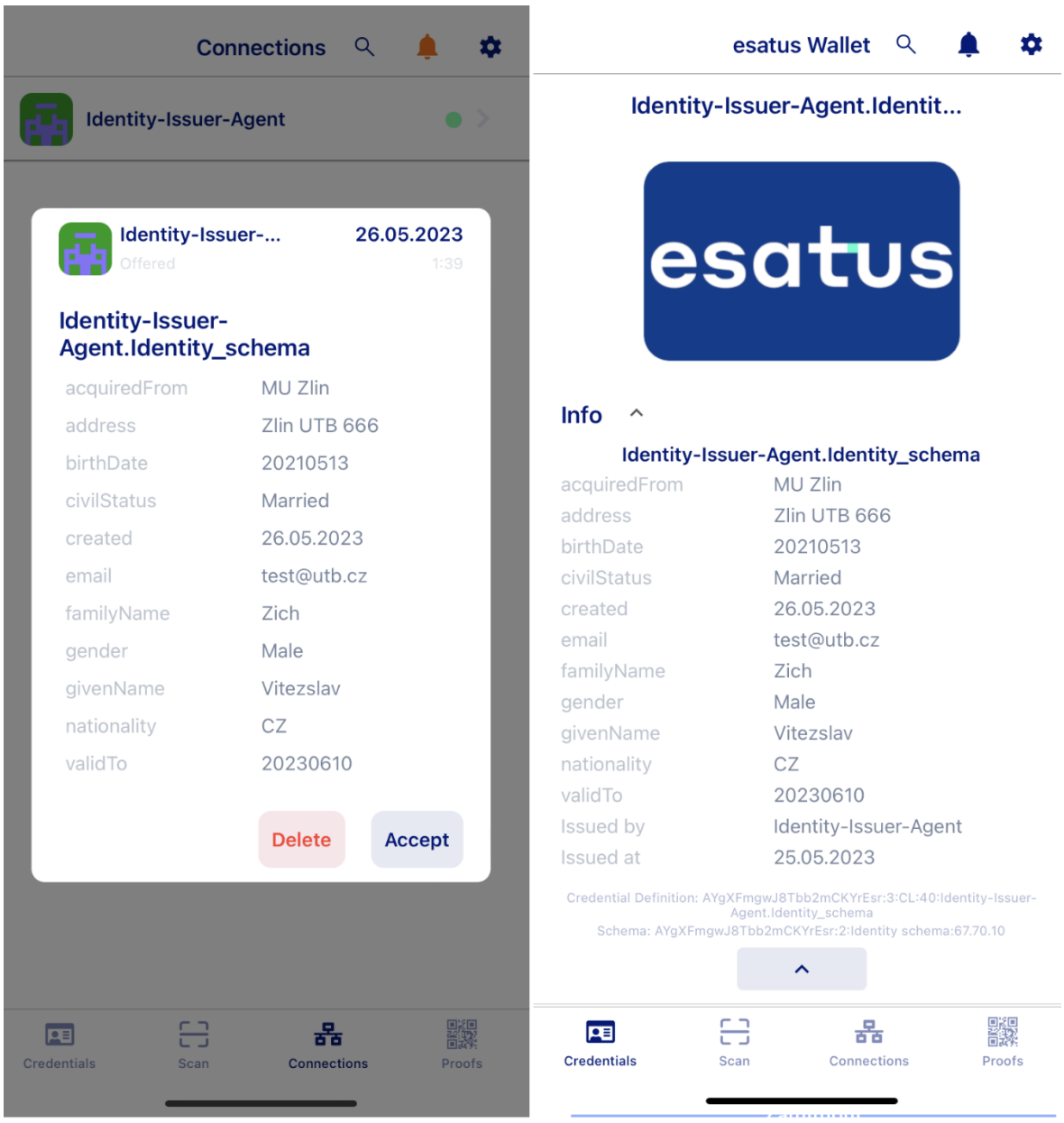


Obrázek 39. Lissi Wallet [66]

6.4.3 Esatus Wallet

Esatus Wallet je podporována jak na iOS tak Android OS, nicméně firma Esatus nabízí kompletní SSI řešení. [58]

Esatus Wallet podporovala navázání spojení, přidání vlastního blockchainu. Nicméně funkční je pouze uložení dokladů. Požadavek na ověření dokladů nebyl úspěšný. V rámci aplikace je potřeba mít funkčně nakonfigurovaný tzv. „gateway server“, což je varianta serveru, který dokáže přeposílat notifikace z ostatních agentů do peněženky.



Obrázek 40. Esatus wallet [66]

6.4.4 BC Wallet

BC Wallet je privátní mobilní peněženka provincie Britská Kolumbie v Kanadě. Po instalaci nenabízí takovou možnost konfigurace jako předešlé testované aplikace. Neobsahuje možnost připojení se na specifický blockchain a je tedy limitovaná pouze pro svou vlastní blockchainovou síť. [59]

6.4.5 Napojení vlastní wallet

Hyperledger Aries zaštiťuje vlastní open source peněženku Aries Bifold, tzv. Aries Mobile agent React Native. Zdrojové kódy je možné si stáhnout, případně provést fork repository. Tímto způsobem byla vytvořena aplikace BC Wallet kterou využívají v produkčním prostředí. Rozhraní je velmi podobné, došlo zde tedy pouze k rebrandingu aplikace. Aktuálně podporuje pouze verzi AIP v 1.0. nicméně verze 2.0. je již v procesu implementace.[60] Zde bych viděl možnost pokračování práce z pohledu provozovatele digitálních peněženek, kdy je třeba řešit nejen mobilní peněženku jako takovou, ale také i zálohování, komunikaci s připojenými agenty, u kterých byly vydány či ověřeny identity, push notifikace, případně obnovu peněženky pomocí mnemotechnické fráze, která je využívána především v oblasti kryptoměn.

7 VYUŽITÍ ŘEŠENÍ V RÁMCI EU

Teoretická část zahrnovala aktuální stav Evropské unie týkající nejen decentralizované identity ale i identity obecně. V rámci této kapitoly budeme diskutovat možnost napojení na evropskou blockchainovou infrastrukturu. Vydefinujeme si aktuální stav v EU, možné limitace a úskalí, která můžeme očekávat.

7.1 EBSI blockchain

EBSI nabízí třetím stranám možnost stát se tzv. „nod operátorem“, což je možnost provozovat jeden z blockchainových nodů pro budoucí evropskou infrastrukturu. Pokud se organizace chce stát součástí EBSI je nutné kontaktovat zástupce European blockchain partnership (EBP) pro daný stát, což je v případě České republiky ministr průmyslu a obchodu Jan Klesla. Kontakt v rámci EBP by měl poskytnout také přehled národních iniciativ, směrem k EBSI, grantů EBSI a další. [61]

EBSI poskytuje vývojová prostředí, pilotní, před produkční a produkční prostředí. Pokud se organizace chce stát součástí EBSI a provozovat svůj vlastní nod, tak je třeba splnit několik podmínek.

V rámci sítě jsou provozovány jak standardní nody, tak i tzv. „validátor“ nody, a jejich práva zda mohou zapisovat či číst z blockchainu mohou být vydána pouze členy EBP.

Po splnění zákonných povinností žadající organizace v rámci své jurisdikce je povolen přístup k pilotní síti EBSI. Pro připojení je nutné také splňovat požadavky EBP, které jsou uvedeny v dokumentu Node Operators Operational Notebook (NOOB).

EBSI následuje tzv. DTAP standard, kdy vývoj softwaru je rozdělen na nasazení do několika prostředí a dbá tak na co nesnažší průběh s minimalizací rizik. Pro objasnění termínu je níže poskytnut popis standardu.

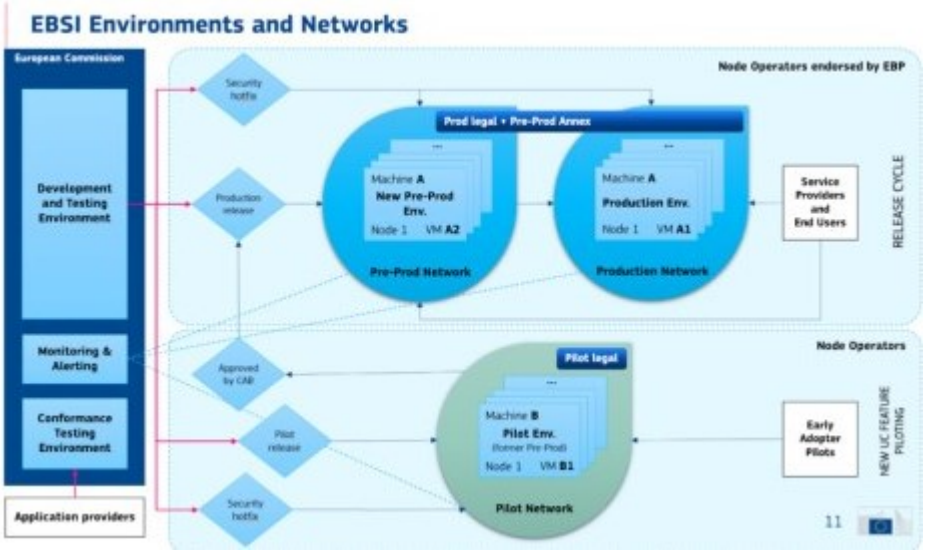
- D – Vývojové prostředí (tzv. dev prostředí) , kde dochází k lokálnímu vývoji nových funkcionalit
- T – Testovací prostředí, pro interní testy funkcionalit, automatizované testy, regresní testy a další
- A – Akceptační prostředí, většinou zde má přístup klient a testuje funkcionality, které jsou připraveny na nasazení do produkčního prostředí
- P – Produkční prostředí, kde běží systémy poskytované zákazníkovi [62]

Jsou zde uvedeny minimální hardwarové požadavky dělící se dle prostředí, kdy každý nod musí mít 3 virtuální hosty s veřejnou IP adresou a přístupem do internetu.

Tabulka 1. Minimální požadavky EBSI [61]

Pilotní prostředí (3xVM)	Předprodukční prostředí (3x VM)	Produkční prostředí (3x VM)
4 vCPU	4 vCPU	8 vCPU
32 GB RAM	32 GB RAM	64 GB RAM
80 GB disk pro OS	80 GB disk pro OS	80 GB disk pro OS
256 GB pro data	256 GB pro data	500 GB pro data
1GB Ethernet lokální síť	1GB Ethernet lokální síť	1GB Ethernet lokální síť
100 Mbit/s Internet a 50ms latence	100 Mbit/s Internet a 50ms latence	100 Mbit/s Internet a 50ms latence

Z pohledu bezpečnosti NOOB dokument vyžaduje konkrétní nastavení firewallu a datacentra v kterých budou tyto nody hostovány musí splňovat normu ISO 27001, která poskytuje rámec pro systémy řízení bezpečnosti informací. Z pohledu nařízení tedy musí nod splňovat uvedenou normu, případně její ekvivalent v rámci jurisdikce státu. Dokument, také poukazuje na procesy, které jsou nutné zavést pro produkční řešení. Jedná se o obecné procesy v rámci EBSI, nicméně také dokument poukazuje na incident reporting, případně proces nasazování nových verzí aplikací. [61]



Obrázek 41. NOOB dokument [61]

EBSI nody poskytují několik protokolů a API, které je možné využít. Hlavní podporovaný protokol je aktuálně Hyperledege Besu na bázi IBFT (Istanbul Byzantine Fault Tolerant) 2.0 konsenzu.

7.2 Agent

V rámci EBSI aktuálně není možné ověřit scénáře a požadavky pro implementaci agentů pro komunikaci s EBSI blockchainem. Scénáře pro komunikaci „Issuer to Holder“ a „Verify“ modul jsou ohlášeny na konci Q2 2023 (informace je aktuální pro květen 2023). [63]

Nicméně už jsou známé DID metody specifické pro EBSI a to konkrétně „DID:le“, což je decentralizovaný identifikátor pro právnické osoby. Tyto identifikátory budou veřejně dostupné prostřednictvím registru DID.

Pro fyzické osoby je vydefinován „DID:np“, který nebude veřejně dostupný, ale bude pseudoanonymizovaný a zároveň veškeré DID dokumenty, týkající se identity budou spravovány digitální peněženkou. Podobná situace je i na poli verifiable credentials, kdy jsou již vydefinovány datové modely pro právnické a fyzické osoby, vysokoškolské diplomy a obecné modely pro akreditace a atestace. [64]

7.3 EU Digital wallet

Evropská digitální peněženka je typ uložiště, v kterém můžete ukládat vaše digitální aktiva, například vaši digitální identitu, digitální certifikáty a další data.

Pro možnost uložení oficiálních evropských dokladů je třeba využívat digitální peněženky splňující určité standardy a funkcionality. Tyto vlastnosti jsou vyhodnocovány podle tzv. Wallet conformance testu (WCT). Jedná se o test, který musí splňovat holder, verifier nebo i issuer. Bez jeho splnění není možné využívat a obecně interagovat s EBSI blockchainem.

V tzv. Compliance reportu jsou uvedeny metody (REST API), které daná peněženka musí volat. Po schválení jsou uvedeni jako „conformanti“. Tim že je ekosystém ve vývoji, tak se mění specifikace i požadavky na funkcionalitu peněženek. Nicméně jak bylo uvedeno v kapitole 7.2 definice pro DID a VC už jsou zdokumentovány.

Aktuálně může instituce požádat pouze o conformance test pro peněženky držitele a issuera. [65]

ZÁVĚR

Diplomová práce se zabývá problematikou využití blockchainových technologií pro decentralizované ověřování identity s aplikací principů „Self-sovereign identity“.

V teoretické části byly nastudovány jednotlivé komponenty a technologie umožňující uvedený koncept využít v praxi. Koncept byl rozdělen na tři hlavní části nutné k probádání tématu. První kapitola byla věnována tématu blockchainu a popisu všech technologií, které umožňují navrhnout robustní decentralizované systémy a zároveň mohou držet status důvěryhodného systému.

Ve druhé kapitole byla popsána a diskutována digitální identita a její modely ověřování. Převažující část kapitoly byla věnována novému konceptu ověřování identity (SSI), který mohl být navržen odborníky díky vzniku důvěryhodných decentralizovaných aplikací postavených na principu blockchainu. Koncept SSI je oproti ostatním typům ověřování identity relativně nový. Bylo tedy nutné probádat i všechny nové technologie a principy, které celý tento ekosystém momentálně tvoří. Součástí celého řešení je využití asymetrické kryptografie veřejných a privátních klíčů, hashování a zero knowledge proof protokolů. Bylo tedy nutné nastudovat především ZKP, jenž je relativně novým pojmem. Z pohledu ochrany osobních údajů a anonymizace je aplikace ZKP velmi zásadním průlomem. Teoretická část také specifikuje, jakým způsobem zabezpečeně propojit všechny účastníky SSI ekosystému. Pomocí konceptu trust triangle, což je základní způsob navazování vztahů a důvěry v SSI spolu s DID a VC.

Třetí kapitola spočívala v ověření aktuálního legislativního rámce na poli identity a blockchainových technologií v Evropské unii, z nichž hlavním prvkem je evropská blockchainová infrastruktura, která spolu s nařízením o evropské digitálním ID bude hlavním hybatelem na poli evropských dokladu a identity v následujících letech.

V praktické části byl tedy úspěšně vytvořen návrh systému s využitím decentralizované identity. Znalosti nabyté v teoretické části byly nezbytné pro korektní navržení celého systému. Jako vrstva důvěry byl zvolen blockchain Hyperledeger Indy, jako SDK pro implementaci agenta Hyperledger Aries. Pro interakci s uživatelem byl implementován web ve Vue3 frameworku komunikující na backend služby napsané v Pythonu. Tyto služby zprostředkovávali pomocí Hyperledger Aries komunikaci s blockchainem i digitálními peněženkami uživatele. Uživatel tedy byl schopný si vytvořit svoji vlastní identitu, ověřit ji pomocí

dat uložených blockchainu a ZKP přes svoji digitální peněženku a získat tím přístup na služby zvolené privátní komunity.

Výstupem práce je tedy návrh a implementace autentizačního mechanismu používající SSI paradigmata. Jeho výhody je možné charakterizovat jak s dopadem na koncového uživatele, tak na provozovatele digitálních služeb. Z pohledu uživatele přináší tento přístup možnost vlastnit vlastní identitu i v rámci digitálního světa, a především možnost se identitou prokazovat s možností sdílení dat pouze s kterými uživatel souhlasí. Zároveň odpadá potřeba používat hesla, protože autentizace probíhá prostřednictvím navázání vztahů a výměny DID dokumentů. Přínosem celé práce je nejen potvrzení SSI jako životaschopného řešení ale i celkového vysvětlení této problematiky na reálných situacích.

Aplikace daného scénáře a řešení z pohledu napojení na evropskou blockchainovou infrastrukturu by bylo možné zejména z pohledu serverových agentů, a to konkrétně „Verifiera“. Na základě ověření dokladu by daný agent už mohl vydávat své komunitní identity, tak jako v implementovaném řešení. Nicméně ještě nejsou známy protokoly a podmínky pro možnost Verifiera v rámci EBSI. Obecně implementace EBSI a evropské digital ID pomůže snížení byrokratické zátěže v Evropské unii.

Potencionální rizika dané implementace jsou především v propustnosti a zátěži daného řešení. Propustnost blockchainových řešení je obecně menší než v centralizovaných řešeních. Je také nutné počítat s výpočetní náročností ZKP, přestože novější metoda zkSTARK má daleko nižší výpočetní náročnost než předchozí implementace.

Pokud vezmeme v potaz potencionální rizika z pohledu uživatele, tak se přenáší zodpovědnost za správu identity právě na uživatele. Bude nutné se o svoji digitální identitu starat, a především vyřešit možné krádeže těchto identit a jak s nimi pracovat. Nicméně klady spojené s decentralizovaným ověřovaním identity jsou daleko větší. Například z pohledu hackerů, se z obrovských honeypotů federovaných a centralizovaných identity služeb, budou muset zaměřit na jednotlivce. Vykradení několik set tisíc identit jedním hackerským útokem nebude možné. Celkově self sovereign identity přístup pro správu identity vyřeší velký počet problémů, které stávající systémy mají a můžeme tedy v nastupujících letech čekat ze strany Evropské unie zásadní novinky pro naši identitu.

SEZNAM POUŽITÉ LITERATURY

[1] BASHIR, Imran. *Mastering Blockchain - Fourth Edition*. 4. Birmingham: Packt Publishing, 2023. ISBN 978-1803241067.

[2] ACHARYA, Vivek, Anand Eswararao YERRAPATI a Nimesh PRAKASH. *Oracle Blockchain Quick Start Guide*. Birmingham: Packt Publishing, 2019. ISBN 978-1789804164.

[3] BARAN, Paul. *On Distributed Communication Networks* [online]. Santa Monica, California: RAND Corporation, 1962 [cit. 2023-05-23]. Dostupné z: https://pages.cs.wisc.edu/~akella/CS740/F08/740-Papers/Bar64.pdf

[4] Lekce 1 - Sítě - Typy používaných sítí. *Itnetwork.cz* [online]. c2023 [cit. 2023-05-23]. Dostupné z: https://www.itnetwork.cz/site/zaklady/site-typy-pouzivanych-siti

[5] INTRODUCTION TO SMART CONTRACTS. *Ethereum.org* [online]. 2022 [cit. 2023-05-23]. Dostupné z: https://ethereum.org/en/developers/docs/smart-contracts/

[6] Learn about Ethereum. *Ethereum.org* [online]. 2023 [cit. 2023-05-23]. Dostupné z: https://ethereum.org/en/learn/

[7] EIP-4361: Sign-In with Ethereum. *Coinsbench.com* [online]. 2022 [cit. 2023-05-23]. Dostupné z: https://coinsbench.com/eip-4361-sign-in-with-ethereum-24a10cef6310

[8] *Hyperledger - Open Source Blockchain Technologies* [online]. c2022 [cit. 2023-05-23]. Dostupné z: https://www.hyperledger.org/

[9] Introduction to Hyperledger Self-Sovereign Identity Blockchain Solutions. *Learning.edx.com* [online]. 2023 [cit. 2023-05-23]. Dostupné z: https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS172x+1T2023

[10] Login With IOTA is Here. *Iota.org* [online]. 2023 [cit. 2023-05-23]. Dostupné z: https://blog.iota.org/login-with-iota-is-here/

[11] Ion - we have liftoff. *Techcommunity.microsoft.com* [online]. 2021 [cit. 2023-05-23]. Dostupné z: https://techcommunity.microsoft.com/t5/security-compliance-and-identity/ion-we-have-liftoff/ba-p/1441555

[12] Polygon ID | Identity infrastructure for Web3. *Polygon.technology* [online]. 2023 [cit. 2023-05-23]. Dostupné z: https://polygon.technology/polygon-id

[13] Why NFTs and SBTs aren't the best solution for digital identity. *Technative.io* [online]. 2022 [cit. 2023-05-23]. Dostupné z: https://technative.io/why-nfts-and-sbts-arent-the-best-solution-for-digital-identity/+

[14] Identity | English meaning. *Dictionary.cambridge.org* [online]. c2023 [cit. 2023-05-23]. Dostupné z: https://dictionary.cambridge.org/dictionary/english/identity

[15] Identity | Glossary CSRC. *Csrc.nist.gov* [online]. 2022 [cit. 2023-05-23]. Dostupné z: https://csrc.nist.gov/glossary/term/identity#:~:text=NIST%20SP%20800%2D79%2D2,CNSSI%204009%2D2015

[16] What is a Digital identity? - Definition from techopedia. *Techopedia.com* [online]. 2012 [cit. 2023-05-23]. Dostupné z: https://www.techopedia.com/definition/23915/digital-identity

[17] Getting Started with Self-Sovereign Identity (SSI). *Learning.edx.org* [online]. 2023 [cit. 2023-05-23]. Dostupné z: https://le arning.edx.org/course/course-v1:Linux-FoundationX+LFS178x+3T2022+

[18] PREUKSCHAT, Alex a Drummond REED. *Self-Sovereign Identity: Decentralized digital identity and verifiable credentials*. Manning, 2021. ISBN 978-1617296598.

[19] Common Federated Identity Protocols: OpenID Connect vs OAuth vs SAML 2. *Securityjourney.com* [online]. 2019 [cit. 2023-05-23]. Dostupné z: https://www.securityjourney.com/post/analysis-of-common-federated-identity-protocols-openid-connect-vs-oauth-2.0-vs-saml-2.0+

[20] MojeID - Přístup ke službám veřejné správy. *Mojeid.cz* [online]. c2023 [cit. 2023-05-23]. Dostupné z: https://www.mojeid.cz/cs/verejna-sprava/

[21] Kim Cameron remembered via his 7 Laws for Identity. *Biometricupdate.com* [online]. 2022 [cit. 2023-05-23]. Dostupné z: https://www.biometricupdate.com/202205/kim-cameron-remembered-via-his-7-laws-for-identity

[22] What is PKI?. *Cpl.thalesgroup.com* [online]. c2023 [cit. 2023-05-23]. Dostupné z: https://cpl.thalesgroup.com/faq/public-key-infrastructure-pki/what-public-key-infrastructure-pki

[23] Decentralized Public Key Infrastructure (DPKI): What is it and why does it matter?. *Hackernoon.com* [online]. 2019 [cit. 2023-05-23]. Dostupné z: https://hackernoon.com/decentralized-public-key-infrastructure-dpki-what-is-it-and-why-does-it-matter-babee9d88579#

[24] The Future of Privacy: Understanding the Different Types of Zero-Knowledge Proofs. *Medium.com* [online]. 2023 [cit. 2023-05-23]. Dostupné z: https://medium.com/coinmonks/the-future-of-privacy-understanding-the-different-types-of-zero-knowledge-proofs-95b49791d4c6

[25] An Exploration of Zero-Knowledge Proofs and zk-SNARKs. *Fisher.wharton.upenn.edu* [online]. 2019 [cit. 2023-05-23]. Dostupné z: https://fisher.wharton.upenn.edu/wp-content/uploads/2020/09/Thesis_Terrence-Jo.pdf

[26] WINDLEY, Phillip. *Learning Digital Identity: Design, Deploy, and Manage Identity Architecture*. O'Reilly Media, 2023. ISBN 978-1098117696.

[27] Decentralized Identifiers (DIDs) v1.0. *W3.org* [online]. 2022 [cit. 2023-05-24]. Dostupné z: https://www.w3.org/TR/did-core

[28] Decentralized Identifiers (DIDs): The Ultimate Beginner's Guide 2023. *Dock.io* [online]. 2023 [cit. 2023-05-24]. Dostupné z: https://www.dock.io/post/decentralized-identifiers

[29] What are Decentralized Identifiers (DIDs)?. [online]. 2022 [cit. 2023-05-24]. Dostupné z: https://www.identity.com/what-are-decentralized-identifiers-dids/

[30] Decentralized Identifier Resolution (DID Resolution) v0.3. *W3c-ccg.github.io* [online]. 2023 [cit. 2023-05-24]. Dostupné z: https://w3c-ccg.github.io/did-resolution/

[31] DID Specification Registries: The interoperability registry for Decentralized Identifiers [online]. 2023 [cit. 2023-05-24]. Dostupné z: https://w3c.github.io/did-spec-registries/#did-methods

[32] The did:keri DID Method [online]. 2023 [cit. 2023-05-24]. Dostupné z: https://weboftrust.github.io/ietf-did-keri/draft-pfeairheller-did-keri.html#name-key-event-log

[33] DIDComm Messaging v2.1 Editor's Draft [online]. 2023 [cit. 2023-05-24]. Dostupné z: https://identity.foundation/didcomm-messaging/spec/v2.1/

[34] Verifiable Credentials Data Model v1.1. *W3C* [online]. 2022 [cit. 2023-05-24]. Dostupné z: https://www.w3.org/TR/vc-data-model/

[35] Verifiable Credentials Framework. *European Commision EBSI* [online]. 2023 [cit. 2023-05-24]. Dostupné z: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/EBSI+Verifiable+Credentials

[36] Verifiable Credentials – how does it work? Understanding key VC principles. *Ubisecure* [online]. 2022 [cit. 2023-05-24]. Dostupné z:

https://www.ubisecure.com/identity-management/verifiable-credentials-understanding-key-principles/

[37] AnonCreds Specification. *Hyperledger AnonCreds* [online]. 2023 [cit. 2023-05-24]. Dostupné z: https://hyperledger.github.io/anoncreds-spec/

[38] Where the W3C Verifiable Credentials meets the ISO 18013–5 Mobile Driving License. *Medium.com* [online]. 2022 [cit. 2023-05-24]. Dostupné z: https://medium.com/@identitywoman-in-business/where-the-w3c-verifiable-credentials-meets-the-iso-18013-5-mobile-driving-license-2b0a6c992920

[39] ISO/IEC 23220-1:2023: Cards and security devices for personal identification — Building blocks for identity management via mobile devices — Part 1: Generic system architectures of mobile eID systems. *Standards.iteh.ai* [online]. 2023 [cit. 2023-05-24]. Dostupné z: https://standards.iteh.ai/catalog/standards/iso/c6163f64-067e-46b0-a69a-c32f3b1067ba/iso-iec-23220-1-2023

[40] Digital ID Wallet: Complete Guide 2023. *Dock.io* [online]. 2023 [cit. 2023-05-24]. Dostupné z: https://www.dock.io//post/digital-id-wallet#countries-with-digital-id

[41] What is eIDAS2 and what changes from eIDAS?. *Mobbeel* [online]. c2009-2023 [cit. 2023-05-24]. Dostupné z: https://www.mobbeel.com/en/blog/what-is-eidas2-and-what-changes-from-eidas/

[42] EIDAS 2: the countdown to a single European Digital ID Wallet has begun. *Thalesgroup.com* [online]. c2023 [cit. 2023-05-24]. Dostupné z: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/identity/eidas-regulations

[43] Jaká jsou Vaše práva v souvislosti s ochranou osobních údajů?. *Právní prostor* [online]. 2018 [cit. 2023-05-24]. Dostupné z: https://www.pravniprostor.cz/clanky/ostatni-pravo/jaka-jsou-vase-prava-v-souvislosti-s-ochranou-osobnich-udaju

[44] Is Europe's MiCA a Template for Global Crypto Regulation?. *Coindesk.com* [online]. 2023 [cit. 2023-05-24]. Dostupné z: https://www.coindesk.com/consensus-magazine/2023/04/20/is-europes-mica-a-template-for-global-crypto-regulation/

[45] The eSSIF-Lab. *The eSSIF-Lab* [online]. 2022 [cit. 2023-05-24]. Dostupné z: https://essif-lab.github.io/framework/docs/essifLab

[46] Experience cross-borders services with EBSI. The first public sector blockchain services in Europe. *European Commision EBSI* [online]. c2023 [cit. 2023-05-24]. Dostupné z: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/

[47] European Blockchain Pre-Commercial Procurement. *European Commision* [online]. 2022 [cit. 2023-05-24]. Dostupné z: https://digital-strategy.ec.europa.eu/en/news/european-blockchain-pre-commercial-procurement

[48] What Is EBSI?. *IOTA* [online]. 2022 [cit. 2023-05-24]. Dostupné z: https://www.iota.org/solutions/ebsi

[49] EBA Structure. *European Blockchain Association* [online]. c2021 [cit. 2023-05-24]. Dostupné z: https://europeanblockchainassociation.org/eba-structure/

[50] VON Network. *Github.com* [online]. 2023 [cit. 2023-05-24]. Dostupné z: https://github.com/bcgov/von-network

[51] Becoming a Hyperledger Aries Developer. *EDX* [online]. 2023 [cit. 2023-05-25]. Dostupné z: https://learning.edx.org/course/course-v1:LinuxFoundationX+LFS173x+1T2023

[52] Default AUTH_MAP Rules. *Github.com* [online]. 2021 [cit. 2023-05-25]. Dostupné z: https://github.com/hyperledger/indy-node/blob/main/docs/source/auth_rules.md

[53] Hyperledger Aries Cloud Agent - Python. *Github.com* [online]. 2023 [cit. 2023-05-25]. Dostupné z: https://github.com/hyperledger/aries-cloudagent-python/

[54] : Hyperledger Aries RFCS. *Github.com* [online]. 2023 [cit. 2023-05-25]. Dostupné z: https://github.com/hyperledger/aries-rfcs/

[55] Hyperledger Aries ACA-Py Docs. *Hyperledger Aries* [online]. 2023 [cit. 2023-05-25]. Dostupné z: https://aca-py.org/main/

[56] Trinsic ID. *Trinsic* [online]. 2023 [cit. 2023-05-26]. Dostupné z: https://trinsic.id/

[57] The Lissi Wallet. *The Lissi Wallet* [online]. 2023 [cit. 2023-05-26]. Dostupné z: https://www.lissi.id/

[58] Esatus SOWL. *Esatus* [online]. 2023 [cit. 2023-05-26]. Dostupné z: https://esatus.com/

[59] BC Wallet. *Province of British Columbia* [online]. 2023 [cit. 2023-05-26]. Dostupné z: https://www2.gov.bc.ca/gov/content/governments/government-id/bc-wallet

[60] About Aries Mobile Agent React Native. *Github.com* [online]. 2023 [cit. 2023-05-25]. Dostupné z: https://github.com/hyperledger/aries-mobile-agent-react-native

[61] EBSI's Node Operators. *European Commision EBSI* [online]. 2023 [cit. 2023-05-25]. Dostupné z: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Node+Operators

[62] DTAP system. *PAQT* [online]. 2023 [cit. 2023-05-26]. Dostupné z: https://paqt.com/en/methods-and-techniques/dtap-system/

[63] EBSI Wallet Conformance Testing. *EBSI Wallet Conformance Testing* [online]. 2023 [cit. 2023-05-26]. Dostupné z: https://api-conformance.ebsi.eu/docs/wallet-conformance

[64] EBSI DID Method. *European Commision EBSI* [online]. 2023 [cit. 2023-05-26]. Dostupné z: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/EBSI+DID+Method#EBSIDIDMethod-EBSIDIDMethod

[65] Wallets. *European Commision EBSI* [online]. 2023 [cit. 2023-05-26]. Dostupné z: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Conformant+wallets

[66] Vlastní zpracování

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AD	Active Directory
AIP	Aries Interop Profile
API	Application Programming Interface
CLI	Comand Line Interface
DAO	Decentralizovaná autonomní organizece
De-Fi	Decentralizované finance
DID	Decentralizovaný identifikátor
DIF	Decentralized Identity Foundation
DLT	Distributed ledger technology
DPKI	Decentralized public key infrastructure
EBA	European Blockchain Assocation
EBP	European Blockchain Partnership
EBSI	European Blockchain Service Infrastructure
EHP	Evropský hospodářský prostor
EIDAS	Electronic IDentification, Authentication and trust Services
EIP	Ethereum Implementation Proposal
EULA	End User License Agreement
EVM	Ethereum Virtual Machine
FIDO	Fast Identity Online
FIM	Federovaný Identity Management
GDPR	General Data Protection Regulation
IBFT	Istanbul Byzantine Fault Tolerant
IDP	Identity Provider
IoT	Internet of Things

MFA	Multifactor Authentication
MiCA	Markets in Crypto-Assets Regulation
NFT	Non-fungible token
NIA	Národní identitní autorita
NIST	National Insitute of Standards and Technology
NOOB	Node Operators Operational Notebook
P2P	Peer to peer
PKI	Public Key Infrastructure
RFC	Request for comments
RP	Relying party
SBT	Soulbound token
SDK	Software developement kit
SSO	Single sing-on
SSI	Self Sovereign Identity
TAA	Transaction Author Agreement
TCP	Transmission Control Protocol
URL	Uniform Resource Locator
VC	Verifiable Credentials
VDR	Verifiable Data Registry
VP	Verifiable Presentation
W3C	World Wide Web Consortium
WCT	Wallet conformance test
ZKP	Zero Knowledge Proof
zkSNARK	Zero-Knowledge Succinct Non-Interactive Argument of Knowledge
zkSTARK	Zero-Knowledge Scalable Transparent Argument of Knowledge

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: OBSAH CD

Adresářová struktura obsahu diplomové práce.

fulltext.pdf:

text diplomové práce ve formátu PDF

prilohy.zip:

- Zdrojové kódy
    - Python implementace teoretické části
    - Python skripty pro backendové služby
    - Vuejs projekt pro frontend
    - Dockerfiles pro rychlé spuštění
    - Hyperledger Aries Cloud Agent knihovna i s kompilačními skripty