Upravljanje samovladne identitete z rešitvijo podjetja Evernym

Nejc Jager[1], Matevž Pustišek[2]

[1]Fakulteta za elektrotehniko, Tržaška cesta 25, 1000 Ljubljana
E-pošta: nejkojager@gmail.com

Managing self-sovereign identity with the help of Evernym

Abstract. *The paper discusses the benefits of self-sovereign identity and the system used for issuing and verifying credentials based on decentralized blockchain networks. This could help universities build a common network within each other and potentially between each other to unify the credentials that the individual institutions are giving out. The system would also be much safer and less likely to be corrupted since the authentication is done on the blockchain network itself.*

1 Uvod

Preden se usedemo na letalo, moramo dokazati, da smo to res mi. Državne ustanove nam izdajo osebne dokumente, s katerimi dokažemo svoje ime, starost, državljanstvo,… Toda iz znanega ali neznanega razloga nam lahko dokazilo o naši identiteti te ustanove odvzamejo. To poimenujemo centraliziran sistem in njegova slabost je ravno ta, da ima avtoriteto, ki ima vso oblast in moč. V popolnem svetu to ne bi bilo problematično, a žal ne živimo v takem svetu. Kaj nam pa lahko ponudi decentraliziran sistem in kaj sploh to je?

Decentraliziran sistem nam lahko ponudi vse, kar nam ponuja centraliziran sistem, poleg tega pa se znebimo pristranske avtoritete. V takem sistemu predstavlja avtoriteto sistem sam, saj vse kar se zgodi, vsaka transakcija, se zabeleži in vsak lahko preveri njeno pristnost. Samovladna identiteta odlično izkoristi prednosti takega sistema, saj namesto, da imamo posamezniki ali organizacije mnogo identitet na različnih (centraliziranih) omrežjih, imamo lahko eno samo identiteto za vsa omrežja. S tem se izognemo zaprtim sistemom in problemom, kako dokazovati svoja znanja, pripadnost, kvalitete, itd. iz enega omrežja v drugega.

Želeli smo poiskati sistem, ki zagotavlja vse gradnike arhitekture samovladne identitete in omogoča seznanjanje s praktično uporabo. Predvsem smo za začetek iskali brezplačne primere podobnih rešitev, ki jih lahko kasneje prilagodimo za svoj primer. Cilj te raziskave je tudi pokazati primer samovladne identitete in kako poenotiti sistem izdaje ter dokazovanja potrdil znotraj univerze in njenih ustanov, kakor tudi kasneje razširiti idejo na celoten državni in mednarodni sistem.

2 Razvoj digitalne identitete

Za razvoj digitalne identitete potrebujemo tri osnovne pogoje [1]: varnost, saj mora biti varovana pred nenamernimi zlorabami in krajo identitete; upravljanje, lastnik identitete mora imeti oblast nad informacijami, ki jih želi deliti; dostopnost, lastnik identitete mora imeti možnost uporabe le te kjerkoli ter kadarkoli.

Da smo prišli do Samovladne identitete, smo šli čez 3 faze pristopov k zagotavljanju identitete [1], [2]: centralizirana, zvezna ter uporabniško osredotočena.

Centralizirana pomeni, da je kontrolirana s strani ene same avtoritete. Na tak način deluje večina spletnih strani in socialnih omrežij, kjer je potrebna registracija. Problem takšnega sistema je v tem, da samo peščica odloča o obstoju in možnosti uporabe naše identitete, saj ni v naši lasti, posledično nam jo lahko kadarkoli vzamejo.

Zvezna identiteta nam omogoča, da je centralizirana identiteta bolj dostopna oziroma prenosljiva. Omogoči nam prijavo z že obstoječimi identitetami drugih ponudnikov, zato ne potrebujemo ustvarjati novih identitet. Primer zvezne identitete je lahko Google račun ali Facebook račun. Mnogo aplikacij pri registraciji ponuja prijavo z elektronsko pošto ter možnosti prijave z Googlom ali Facebookom. Deluje na principu Single sign-on ali SSO (slo. Enkratni vpis), ki omogoča, da se lahko posameznik prijavlja v različne sisteme z istim računom oziroma identiteto [3]. Težava centraliziranosti pa še vedno ostaja pri identitetah s katerimi se prijavljamo, poleg tega pa problem predstavlja tudi zasebnost, saj ima avtoriteta zvezne identitete v svoji bazi podatke o prijavah na določenih straneh, kar lahko izrabi sebi v prid.

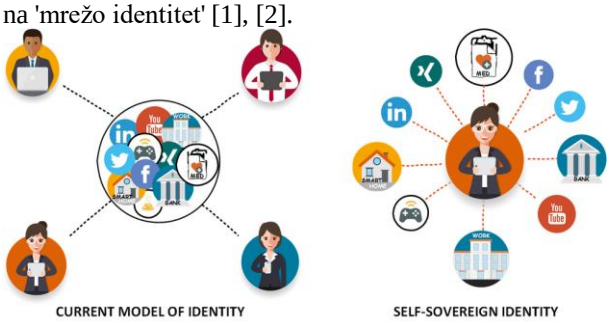
Tretji pristop je uporabniško osredotočen, bolje rečeno uporabniško naravnan. Uporabnik si ustvari identiteto in s tem ima samo on kontrolo nad svojo identiteto, sam izbira, katere informacije bo delil s kom, ima več pravic in odgovornosti. Imamo dva primera uporabniško naravnanih rešitev. Prva je OpenID, kjer za ustvarjanje računa potrebuješ ponudnika, s čimer nismo rešili centraliziranosti, ker so ponudniki avtoritarni. Druga rešitev pa je Facebook Connect, kar že iz prejšnjega pristopa lahko sklepamo, da nismo skoraj nič napredovali.

Vse naštete probleme prejšnjih pristopov lahko rešimo s samovladno identiteto.

3 Samovladna identiteta

Samovladna identiteta (angl. Self-sovereign identity ali SSI) je decentralizirana, varna, kjerkoli dostopna rešitev za samoupravljanje z lastno identiteto. Noben ne more vzeti drugemu digitalne identitete. Omogoča ti dodajanje in deljenje določenih atributov, ne nujno vseh naenkrat, zgolj tistih, ki jih potrebuješ. Pred tem smo imeli tudi težavo z dostopnostjo, saj je vsaka organizacija hranila identitete pri sebi, tukaj jo hrani

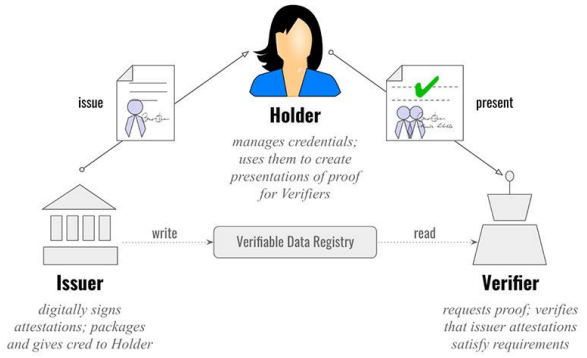
lastnik sam in s tem se lahko kamorkoli kadarkoli poveže. Tudi organizacije med sabo se lahko tako lažje povežejo, saj ne rabijo povezovat svoja 'skladišča' informacij med seboj, ampak se lahko zgolj priključijo na 'mrežo identitet' [1], [2].



Slika 1. Razlika med trenutnim in SSI pristopom. Vir: https://labs.hypersign.id/posts/ssi-detail/

Eden od ključnih gradnikov SSI je blockchain omrežje, saj nam zagotavlja decentraliziranost. Preko njega se izvajajo transakcije, ki se beležijo na verigo blokov in prispevajo k transparentnosti. Posameznik in organizacije potrebujejo tudi svoje digitalne denarnice za shranjevanje in deljenje potrdil ter atributov. Primerno je tudi, da imajo izdajatelji potrdil lahko dostopne spletne strani oziroma aplikacije, kjer lahko zahtevaš potrdila.

Vloge v sistemu samovladne identitete so zelo preproste: izdajatelj, imetnik ter overjavitelj potrdil [4].



Slika 2. Vloge samovladne identitete in njihove povezave. Vir: https://gitlab.com/evernym/verity/verity-sdk/-/tree/main#verity-sdk

3.1 Tehnologija razpršene evidence

Tehnologija razpršene evidence (angl. Distributed ledger technology ali DLT) je skupek sinhroniziranih informacij, ki so razpršeno deljene in replicirane po svetu. Ker so te informacije na več lokacijah hkrati, ki niso upravljane znotraj zgolj ene organizacije, jim pravimo decentralizirane.

S to tehnologijo informacije in identitete niso centralno upravljane, zato je dobra podlaga za samovladno identiteto.

3.2 Decentraliziran identifikator

Decentraliziran identifikator (angl. Decentralized identifier ali DID) je globalni identifikator, ki nima centralizirane avtoritete, ki bi skrbela za njegovo kontrolo. Nadzor se dela s kriptografijo. Njegov namen je zagotoviti varen prenos informacij med entitetami [4], [5].

3.3 Preverljivo dokazilo

Preverljivo dokazilo (angl. Verifiable Credential ali VC) je dokazilo, ki je digitalno podpisano in s tem preverljivo. V analognem svetu je lahko dokazilo z žigom in podpisom ponarejeno. Kako se temu izogniti v digitalnem svetu? Izdajatelj dokazil digitalno podpiše določeno dokazilo in ga izda imetniku. Transakcija se izvede in zapiše na verigo blokov. Overjavitelj nato preveri potrdilo tako, da preveri njegov digitalni podpis. Preveri ga z izdajateljevim javnim ključem, saj je bil digitalni podpis narejen s privatnim [4], [5].

3.4 Izdajatelj potrdil

Izdajatelj potrdil (angl. Issuer) je posameznik ali organizacija, ki izda dokazilo določeni identiteti. Izdajatelj mora ustvariti shemo in credential definition s katerima določi, katere in kakšne atribute bo vsebovalo dokazilo, ki ga bo kasneje izdajal [4]. Atributi bodo isti, njihova vsebina se pa spremeni glede na to, komu je dokazilo namenjeno. Potrdila so digitalno podpisana.

3.5 Overjavitelj potrdil

Overjavitelj potrdil (angl. Verifier) zahteva od identitete potrdilo in ga preveri, če je veljavno. Preveri digitalni podpis in ujemanje poslanega dokazila oziroma atributov, katere ima imetnik v lasti. Overjavitelj lahko prebere kdo je izdajatelj potrdila, komu je bilo izdano, ali je bilo spremenjeno od časa izdaje in ali je bilo zavrnjeno [4].

3.6 Imetnik potrdil

Imetnik potrdil (angl. Holder) prejme potrdila od izdajatelja in jih deli z overjaviteljem. S samovladno identiteto ima imetnik neposredno povezavo med izdajateljem in overjaviteljem, brez posrednikov [4]. Svoja potrdila in njihove atribute hrani v digitalni denarnici.

3.7 Digitalna denarnica

Digitalna denarnica je aplikacija (spletna stran ali podaljšek (angl. Extension)), ki zagotavlja uporabniku shranjevanje, upravljanje in deljenje svojih digitalnih potrdil.

4 Sovrin

Fundacija Sovrin je neprofitna organizacija, ki upravlja z omrežjem, na katerem so povezani SSI-ji [6]. To je le eden od ponudnikov SSI rešitev, obstajajo tudi drugi kot na primer uPort, Hypersign,… [5] Sovrin ponuja MainNet (glavno omrežje), kjer se organizacije in posamezniki lahko povežejo med seboj in tudi integrirajo aplikacije s SSI podporo. Ponujajo še StagingNet in BuilderNet, ki sta za predprodukcijsko in razvijalsko fazo projektov. Omrežje Sovrin deluje na Hyperledger Indy [6].

Na njihovi spletni strani so objavljeni različni primeri uporabe omrežja Sovrin, med drugim tudi rešitev izdaje digitalnih potrdil podjetja Evernym.

4.1 Hyperledger Indy

Hyperledger Indy predstavlja igrišče za razvijanje programske opreme za povezovanje s SSI. Uporablja odprtokodni DLT. Na tako imenovanih 'ledgerjih' so shranjene transakcije in podatki. 'Ledgerji' so razpršeni in sinhronizirani, torej decentralizirani [7], [8], [9].

Na GitHubu imajo celo zbirko dokumentacije ter priročnikov, kako vzpostaviti povezavo in kreirati identiteto. V samem začetnem konceptu omenijo primer: Alice je zaključila šolanje in je dobila potrdilo o končanem šolanju, želi se zaposliti in kasneje zaprositi banko za posojilo. Recimo, da ima Alice svoj SSI. Šola ji ob koncu šolanja pošlje potrdilo o končanem šolanju. Ko se prijavi na delo, lahko določene atribute končanega šolanja pošlje delodajalcu, kot potrdilo o svojem znanju in kompetencah. Ko se zaposli, dobi potrdilo o zaposlenosti, ki ga lahko izkoristi za prijavo za posojilo pri banki. Ker so vse te transakcije na 'ledgerju', torej jih lahko res preverimo, da so se zgodile, so tudi podatki, ki smo jih delili z drugimi, zaupanja vredni [8].

5 Evernym

Veliko organizacij je implementiralo SSI v aplikacije, na primer aplikacije za covid potrdila za letališča ter druge ustanove ali pa aplikacije za potrdila o študiju, ki jih lahko uporabiš kasneje za prijave na delo. Evernym je ena izmed teh organizacij, ki je ponudila končno rešitev ter primere aplikacij za izdajo ter preverjanje potrdil, hkrati pa je implementirala SSI v digitalno denarnico, ki si jo lahko naložiš na telefon [10].

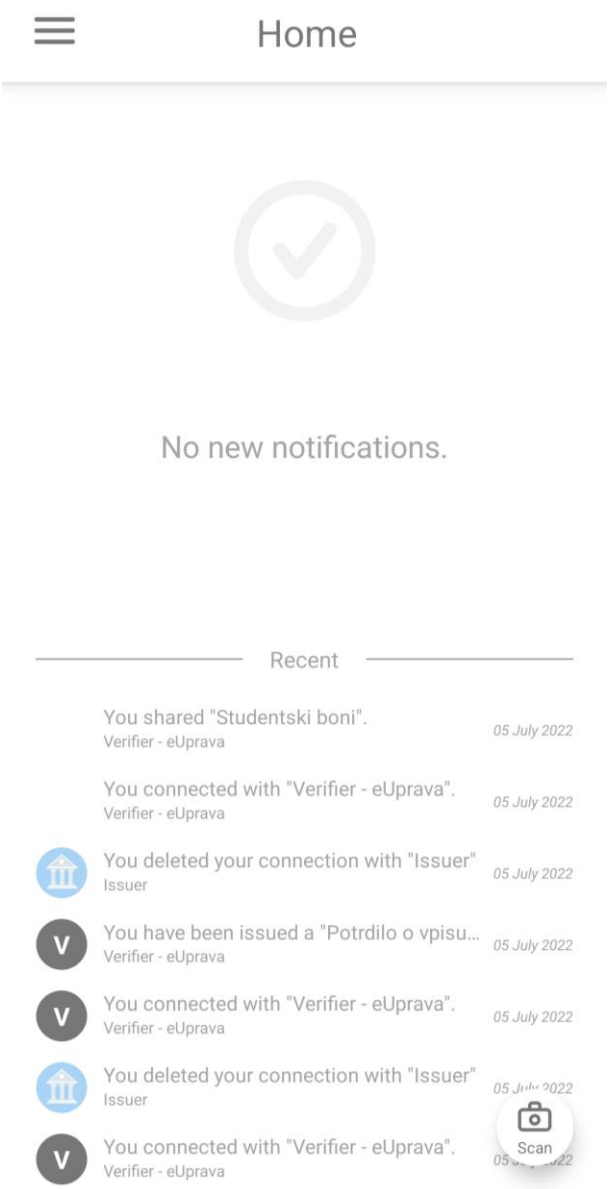
5.1 Verity

Verity je aplikacija za izdajo preverljivih dokazil. Zgrajena je sicer na Hyperledger Aries, ki je bolj namenjen za izdajo potrdil, vendar njihova digitalna denarnica pa je povezana z Indy 'ledgerjem'. Njen namen je predvsem omogočiti organizacijam, da igrajo vlogo izdajatelja in overjavitelja potrdil. Dela se lahko lotimo na 2 načina, z Verity SDK (angl. Software development toolkit) ali pa z Verity REST API. Verity SDK omogoča enostavno integracijo izdajanja in overjanja potrdil v lasten projekt oziroma aplikacijo. SDK im na voljo pisanje v Javi, NodeJs, Pythonu ali .NET. Primer kode lahko zaženeš lokalno ali s pomočjo Dockerja. Prednost tega načina je tudi, da lahko spišeš svojo shemo in definicijo dokazila. Shema je ogrodje s katerim definiramo atribute, ki jih bo shema vsebovala. Definicija dokazila vsebuje podatke, ki jih vstavimo v shemo pod izbrane atribute, torej CD (angl. Credential definition) mora ustrezati shemi. Če imamo shemo za izdajo potrdila o vpisu, imamo atribute, kot so datum vpisa, stopnja šolanja, ime in priimek, datum rojstva itd. Prav tako moramo vse te atribute zapolniti s podatki, ki jih zapišemo v CD.

Druga možnost je REST API, s katero smo se lotili dela mi. Za to potrebujemo DomainDID in APIkey, ki ju lahko sami ustvarimo ali pa dobimo od Evernyma.

5.2 Connect.me

Connect.me je digitalna denarnica podjetja Everynm, ki se uporablja za shranjevanje in izdajo potrdil. Prijavi se lahko zgolj 1 uporabnik na napravo, deluje kot samostojna aplikacija [11].



Slika 3. Connect.me začetna stran.

5.3 Primer izdajatelja

Preden identiteta prejme dokazilo, se mora vzpostaviti varna povezava med njo in izdajateljem. Ustvari se povezovalni DID, ki ga zapakiramo v QR kodo in optično preberemo s Connect.me denarnico, kamor se tudi shrani povezava. Povezava med identiteto in izdajateljem je tudi svoj DID, saj s tem zagotovimo, da je možna le ena povezava med njima. Po uspešni povezavi se prenese dokazilo imetniku identitete [12].

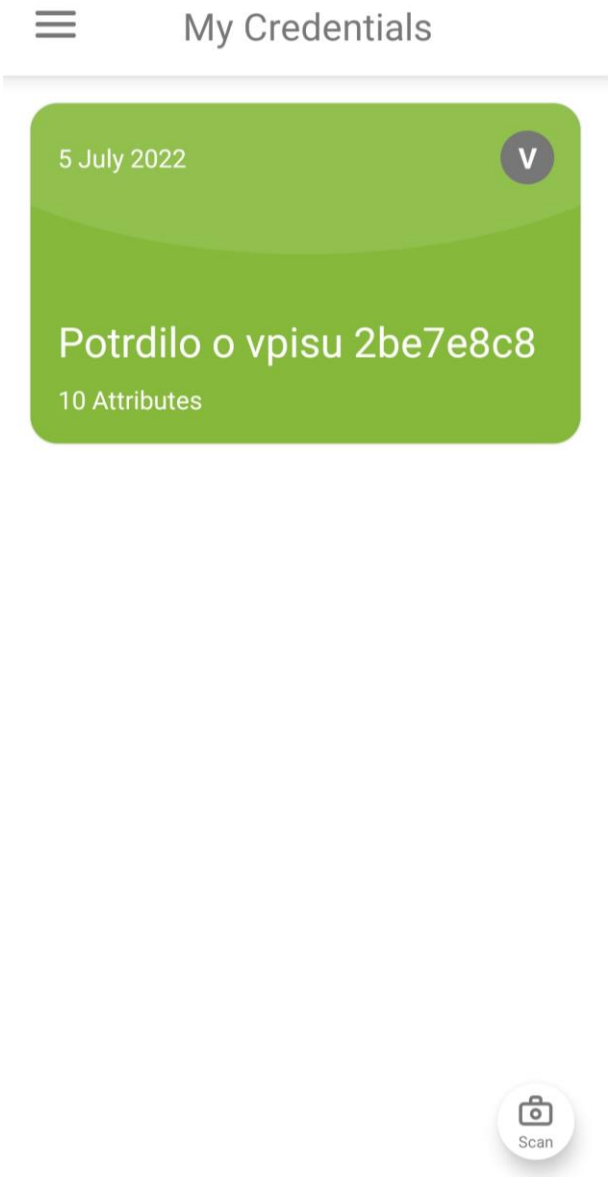
5.4 Primer overjavitelja

Pri overjavitelju pa se najprej vzpostavi povezava kot pri izdajatelju, torej povezovalni DID, potem pa se zahteva potrdilo. Imetnik deli potrdilo oziroma

določene atribute, ki jih overjavitelj zahteva, ta pa glede na njihovo verodostojnost izbrano dokazilo potrdi ali pa zavrne [13].

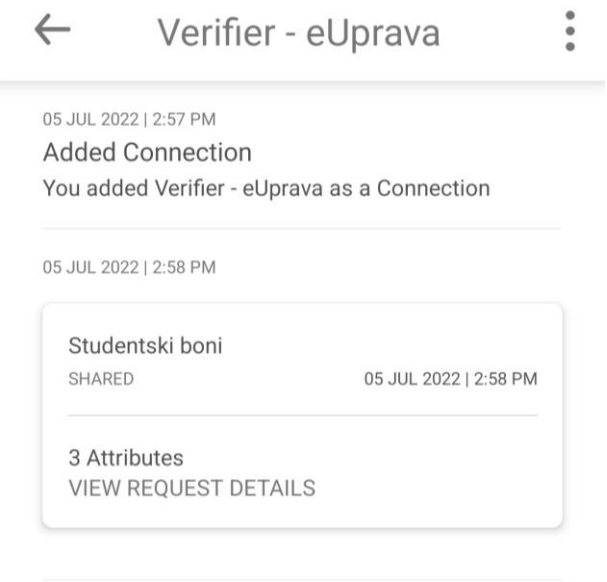
6 Primer rešitve za univerzo

Lotili smo se rešitve za Univerzo v Ljubljani s pomočjo Evernyma in njihovih primerov. Študent bi si ustvaril svoj SSI ter naložil digitalno denarnico na svoj telefon. Fakulteta bi mu izdala potrdilo o vpisu, potrdilo o zaključenih predmetih, predmetniku, določena priznanja in podobno. Študent bi vse te atribute delil za pridobitev štipendije, študentskih bonov, odobritve prepisa, študija v tujini, zamenjave, ter konec koncev tudi prijave na delo.



Slika 4. Potrdilo o vpisu z nekaterimi atributi.

Napisane primere smo adaptirail na način, da imamo izdajatelja Fakulteto za elektrotehniko, ki nam pošlje potrdilo o vpisu in njene atribute. Potem smo za overjavitelja izbrali študentske bone, ki ne potrebujejo vseh atributov iz potrdila o vpisu, le nekatere in te smo tudi delili.



Slika 5. Deljenje atributov.

7 Zaključek

Samovladna identiteta in njena implementacija lahko reši probleme centraliziranosti, omejitve z dostopnostjo ter potencialne nevarnosti pred krajo/izgubo identitete. S tem projektom smo zgolj prikazali primer rešitve, ki pa ni tako daleč od konkretnega sistema, ki bi deloval na nivoju univerze.

Evernym ima dobro zasnovano rešitev, njena implementacija nam je nekajkrat predstavljala težavo, ker so navodila delovala malo preohlapna, inženirju ali programerju pa verjetno ne bi smela predstavljati prevelikih težav.

Samovladna identiteta je rešitev v pravo smer k zagotavljanju identitet, s katerimi lahko pridobivamo in delimo dokazila, saj imamo vsa potrebna dokazila na

enem mestu in v digitalni obliki, namesto da iščemo potrdila po predalih in registratorjih ter delamo kopije potrdil. Vsekakor se lahko primer rešitve za univerzo razširi na državni ali kar svetovni nivo, bo pa pri odpravi fizičnih potrdil treba zagotoviti močno digitalno pismenost.

Literatura

[1] A. Tobin, D. Reed, F. P. J. Windley, in S. Foundation, „The Inevitable Rise of Self-Sovereign Identity“, str. 24, 2017.

[2] „The Path to Self-Sovereign Identity“. http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html (pridobljeno 24. julij 2022).

[3] V. Radha in D. H. Reddy, „A Survey on Single Sign-On Techniques“, *Procedia Technol.*, let. 4, str. 134–139, 2012, doi: 10.1016/j.protcy.2012.05.019.

[4] „Files · main · Evernym / Verity / Verity SDK · GitLab“, *GitLab*. https://gitlab.com/evernym/verity/verity-sdk/-/tree/main (pridobljeno 24. julij 2022).

[5] „In depth introduction to Self Sovereign Identity (SSI)“, 14. junij 2020. https://labs.hypersign.id/posts/ssi-detail/ (pridobljeno 24. julij 2022).

[6] „Home“, *Sovrin*. https://sovrin.org/ (pridobljeno 24. julij 2022).

[7] „Hyperledger Indy – Hyperledger Foundation“. https://www.hyperledger.org/use/hyperledger-indy (pridobljeno 24. julij 2022).

[8] „Indy SDK“. Hyperledger, 23. julij 2022. Pridobljeno: 24. julij 2022. [Na spletu]. Dostopno na: https://github.com/hyperledger/indy-sdk/blob/1c7096dd95d0fd53881070f66907df4b9e61b874/docs/getting-started/indy-walkthrough.md

[9] „What Is Hyperledger Indy?“, *Sovrin*. https://sovrin.org/faq/what-is-hyperledger-indy/ (pridobljeno 24. julij 2022).

[10] „Evernym | The Self-Sovereign Identity Company“, *Evernym*. https://www.evernym.com/ (pridobljeno 24. julij 2022).

[11] „Connect.Me“, *Evernym*. https://www.evernym.com/connectme/ (pridobljeno 24. julij 2022).

[12] „docs/howto/How-to-build-Issuer-using-REST-API.md · main · Evernym / Verity / Verity SDK · GitLab“, *GitLab*. https://gitlab.com/evernym/verity/verity-sdk/-/blob/main/docs/howto/How-to-build-Issuer-using-REST-API.md (pridobljeno 24. julij 2022).

[13] „docs/howto/How-to-build-Verifier-using-REST-API.md · main · Evernym / Verity / Verity SDK · GitLab“, *GitLab*. https://gitlab.com/evernym/verity/verity-sdk/-/blob/main/docs/howto/How-to-build-Verifier-using-REST-API.md (pridobljeno 24. julij 2022).