Samoupravljana digitalna identiteta na verigi blokov Cardano

Nikolay Vasilev, Dejan Lavbič
Univerza v Ljubljani, Fakulteta za računalništvo in informatiko, Večna pot 113, 1000 Ljubljana
nv7834@student.uni-lj.si, dejan.lavbic@fri.uni-lj.si

Izvleček

Problem današnjega interneta je, da je na voljo veliko informacij, ki jih nekdo nadzoruje (npr. oseba, organizacija), teh ljudi pa sploh ne poznamo. Samoupravljana identiteta je okvir zaupanja, pri katerem imajo entitete, kot so: ljudje, organizacije in abstraktne entitete, svoje popolnoma avtonomne identitete. Ta vrsta decentraliziranih digitalnih identitet s pomočjo decentraliziranih identifikatorjev in preverljivih poverilnic entitetam omogoča varno komunikacijo, nadzor nad lastnimi podatki ter izbiro, kaj in s kom bodo delili. Izmenjava podatkov se zgodi z uporabo verige blokov in tehnologije razpršene evidence, ki nam omogoča zaščitene in varne transakcije. S pomočjo te nove tehnologije in verige blokov Cardano smo razvili odprtokodno rešitev, ki bo študentom v pomoč pri izobraževalnem procesu. Ta rešitev pomaga predstaviti funkcionalnosti, ki nam jih decentralizirane digitalne identitete ponujajo pri izobraževanju. Z uporabo SWOT-analize smo primerjali sistem z že obstoječimi rešitvami, pri čemer pokažemo, da uporaba samoupravljene digitalne identitete naredi našo rešitev varnejšo, zmogljivejšo, cenejšo in uporabnejšo.

Ključne besede: decentralizirana digitalna identiteta, decentraliziran identifikator, samoupravljana identiteta, preverljiva poverilnica, preverljiva predstavitev, veriga blokov Cardano

SELF-SOVEREIGN DIGITAL IDENTITY ON THE CARDANO BLOCKCHAIN

Abstract

Nowadays, there is a problem on the Internet with the overabundance of information controlled by a single entity (e.g. person, organization), which we don't know at all. Self-sovereign identity is a framework of trust where entities such as people, organizations, and abstract entities, have their own fully autonomous identities. With the help of decentralized identifiers and verifiable credentials, this type of decentralized digital identity enables entities to securely communicate, control their data, and choose what and with whom to share. Data exchange occurs using a blockchain and a distributed ledger technology, which allows for protected and safe transactions. With the help of this new technology and the Cardano blockchain, we have developed an open-source solution to help students in their educational process.
This solution allows us to present the decentralized digital identities' functionalities in education. Using SWOT analysis, we compared the system to existing solutions, proving that self-sovereign digital identity makes our solution more secure, robust, cheaper, and practical.

Keywords: Decentralized digital identity, decentralized identifier, self-sovereign identity, verifiable credential, verifiable presentation, Cardano blockchain

1 UVOD

Zaradi naraščajoče potrebe po digitalnih identitetah (*angl.* Digital identity) [4, 9] se je zanimanje za upravljanje z identitetami v zadnjih letih povečalo. Digitalna identiteta je velik del življenj ljudi na spletu in se večinoma uporablja kot digitalni dokaz, da je lastnik tisti, za katerega se predstavlja, ko komunicira s storitvami.

Upravljanje identitet na spletu lahko najbolje predstavimo s tremi modeli, ki so se z leti razvijali in dopolnjevali [10, 12]. Prvi model identitete, ki je najbolj znan in že dolgo časa uporabljan s skoraj vsemi identifikatorji in poverilnicami, je centraliziran model identitete (*angl.* Centralized identity model) [6]. Tovrstne digitalne identitete se vzpostavijo z ustvarjanjem računa na spletnem mestu, storitvi ali aplika-

ciji. To pomeni, da entitetam neki drug centraliziran organ posoja poverilnice, ki omogočajo omejen nadzor in dovoljenja, vendar na koncu te poverilnice še vedno pripadajo organu, ki jih je izdal. Entitete ne morajo obstajati v tem centraliziranem sistemu, če nimajo ustvarjenega uporabniškega računa. Zato je možnost dostopa do storitev preklicana, ko entiteta izbriše vse svoje račune, povezane s tem centraliziranim ponudnikom. Druge težave tega modela so naslednje: vsaka spletna stran izvaja svoje varnostne politike in politike o zasebnosti, ki se med seboj razlikujejo; podatki o identiteti niso prenosljivi ali ponovno uporabni; upravljanje vseh različnih računov (uporabniških imen in gesel) je težko in lahko postane breme za entiteto; centralizirane baze podatkov lahko povzročijo resne kršitve varnosti osebnih podatkov. Drugi model identitete, imenovan model federativne identitete (*angl.* Federated identity model) [22], odpravi nekatere težave centralizirane identitete. Izboljšava je, da je med entiteto in centraliziranim ponudnikom dodan ponudnik identitete (*angl.* Identity provider, IDP). Tako ima lahko entiteta en uporabniški račun pri IDP, kar bo omogočilo skupno uporabo nekaterih osnovnih podatkov o identiteti v katerem koli spletnem mestu, storitvi in aplikaciji, ki uporablja ta IDP. Obstaja veliko znanih in uspešnih protokolov, ki uporabljajo ta identitetni model (SAML, OAuth, OpenID Connect), vendar ima tudi ta model nekaj resnih težav, kot so: še vedno obstaja težava, da je treba imeti več kot en račun (identiteta), saj ne obstaja le en IDP, ki bi deloval z vsemi spletnimi mesti, storitvami in aplikacijami; uporabniki morajo zaupati upravljanje in nadzor svojih podatkov nekomu (IDP), ki ga sploh ne poznajo; računi niso bolje prenosljivi kot računi centralizirane identitete; tudi ponudniki identitet uporabljajo centralizirano bazo podatkov, kar pomeni, da podatki niso zaščiteni proti kibernetskim napadom, zato IDP tudi onemogoča uporabnikom, da bi lahko varno delili nekatere svoje najpomembnejše osebne podatke. Najnovejši model – model decentralizirane identitete (*angl.* Decentralized identity model) – ne temelji več na uporabniških računih, vendar deluje kot identiteta v resničnem svetu. Ta model temelji na neposrednem odnosu med dvema entitetama (vrstnikoma), zato se komunikacija imenuje »Vsak z vsakim« (*angl.* Peer-to-peer, P2P). Tako decentralizirane identitete dajejo entiteti popolno avtonomijo nad lastno identiteto, ki je lahko podprta z uporabo verige blokov (*angl.* Blockchain) [2] in tehnologije razpršene evidence (*angl.* Hyperledger technology) [1], tako da si oba vrstnika delita povezavo, ki je zavarovana z uporabo decentralizirane infrastrukture javnih ključev (*angl.* Decentralized Public Key Infrastructure, DPKI) [7]; javni ključi se izmenjajo za omogočanje zasebnih in varnih povezav med dvema vrstnikoma; nekateri izmed teh javnih ključev so shranjeni v javnih verigah blokov za preverjanje podpisov na poverilnicah.

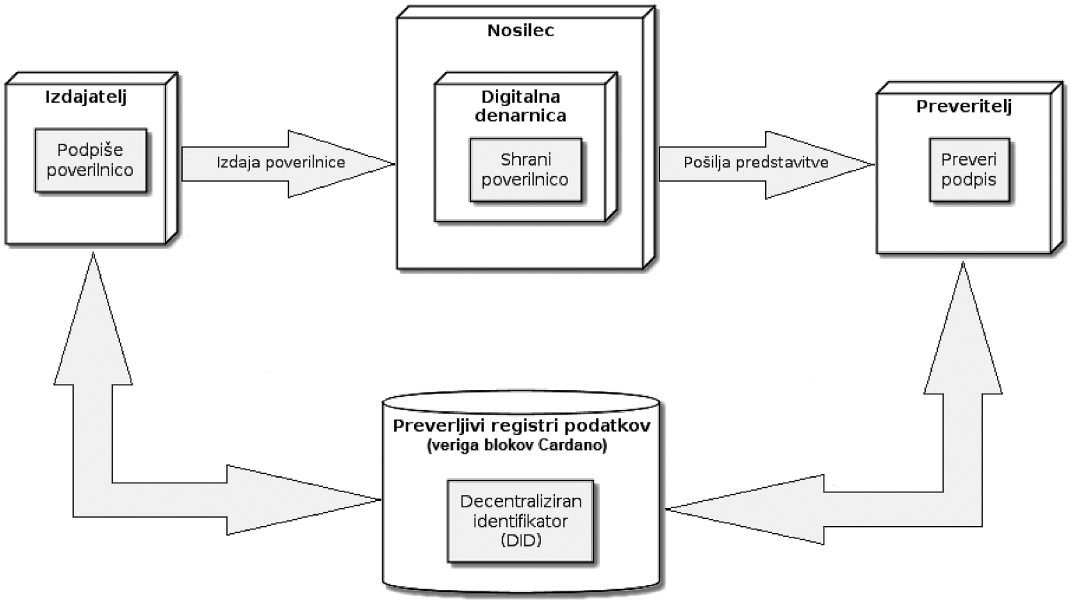
Vrsta decentralizirane identitete je samoupravljana identiteta (*ang.* Self-sovereign identity, SSI) [12, 17], ki vpeljuje tudi decentralizirane identifikatorje (*angl.* Decentralized identifier, DID) [19] in preverljive poverilnice (*angl.* Verifiable credential, VC) [20], ki imajo naslednjo vlogo: decentralizirani identifikatorji omogočajo varno komunikacijo med entitetami; entitete si izmenjujejo preverljive poverilnice prek že ustvarjenega varnega komunikacijskega kanala na tak način, da lahko entitete nadzorujejo svoje osebne podatke in izbirajo, kaj in s kom bodo delile. Da bi predstavili, kako samoupravljane identitete obvladujemo v praksi in predvsem pri izobraževanju, bomo razvili primer uporabe za podporo študentom med študijskim procesom, ki bo uporabljal SSI na verigi blokov Cardano. Študenti morajo zelo pogosto znati: upravljati s svojimi osebnimi informacijami, dokazovati svojo identiteto ter varno in hitro opravljati svoje obveznosti.

Čeprav je že veliko razvitih sistemov, ki študentom pomagajo pri tem, se bomo osredinili na manjkajoče dele teh rešitev in jih z implementacijo SSI nadgradili. Analiza sistema in primerjava z drugimi podobnimi rešitvami s pomočjo SWOT-analize nam bo pomagala ugotoviti, kaj nam implementacija SSI omogoča, kaj so njene slabosti in kaj še lahko izboljšamo. Tako lahko ocenimo uporabnost SSI kot tehnološke rešitve na izbrani problemski domeni.

V razdelku 2 tega prispevka bomo opisali, kaj predstavljajo SSI na splošno, katere so njene najpomembnejše komponente in kakšna je njihova arhitektura. Razdelek 3 se bo začel z opisom že obstoječih sistemov in s predstavitvijo, kako nam bodo pomagali pri razvoju naše rešitve; opisali bomo celotno kompleksnost naše rešitve. V razdelku 4 sledita predstavitev glavnih funkcionalnosti odprtokodne rešitve in ovrednotenje naše rešitve s pomočjo SWOT-analize. V razdelku 5 bomo povzeli rezultate analize, predlagali možne nadgradnje tehnologije in predstavili razpon njene potencialne uporabe v prihodnosti.

2 SAMOUPRAVLJANA IDENTITETA

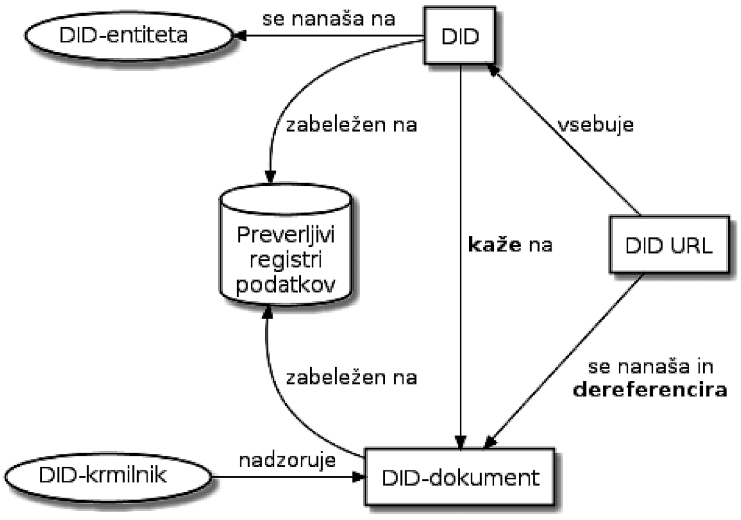
Samoupravljana identiteta je okvir zaupanja, pri katerem imajo entitete, kot so: ljudje, organizacije in abstraktne entitete, svoje identitete. Ta vrsta decentraliziranih digitalnih identitet s pomočjo decentraliziranih identifikatorjev in preverljivih poverilnic entitetam omogoča varno komunikacijo, nadzor nad lastnimi podatki ter izbiro, kaj in s kom bodo delili. DID uporabnikom omogoča vzpostavitev varnega komunikacijskega kanala z uporabo decentralizirane infrastrukture javnih ključev. Ko je kanal vzpostavljen, lahko entitete izmenjajo preverljive poverilnice, ki lastnikom omogočajo nadzor nad svojo identiteto oziroma nad osebnimi podatki. VC dejansko predstavljajo globalno enolične zahtevke izdajatelja o nekom ali nečem drugem. Da bi lahko entitete dobile nadzor nad lastnimi podatki oziroma možnost izbrati, katere podatke bodo delile (podatke iz ene ali več poverilnic), je W3C (*angl.* World Wide Web Consortium) [21] predlagal preverljive predstavitve (*angl.* Verifiable presentation, VP) [20]. VP predstavlja dokaz, da ima entiteta preverljive poverilnice (podatke) za določene trditve, oziroma omogoča entitetam izbrati, katere svoje poverilnice (zahtevke) in s kom jih bodo delile. Kot je prikazano na sliki 1, VC in VP omogočata dokazovanje in preverjanje podatkov ter sta glavni del SSI-arhitekture oziroma sta glavni del komunikacije med izdajateljem (*angl.* Issuer), nosilcem (*angl.* Holder) in preveriteljem (*angl.* Verifier). V naši rešitvi so preverljivi registri podatkov verige blokov Cardano, ki uporabnikom omogočajo zaščitene in varne transakcije; izdajatelji in preveritelji so profesorji in asistenti, čeprav je lahko vsaka entiteta, ki ima svoj DID, objavljena na verigi blokov; nosilci pa so študenti, ki potrebujejo le svojo digitalno denarnico za zbiranje in deljenje svojih poverilnic.



Slika 1: **Glavne vloge pri SSI-arhitekturi**

V rešitvi bomo implementirali DID skladno s standardom W3C [19] na verigi blokov Cardano. Kot opisuje standard, je nekaj glavnih konceptov, s katerimi se srečamo, ko govorimo o arhitekturi DID (slika 2):

- **DID:** globalno enolični identifikator oziroma enotni identifikator vira (*angl.* Uniform Resource Identifier, URI), ki kaže na DID-dokument in je sestavljen iz treh delov (primer 1). DID je objavljen na verigi blokov, da lahko uporabnikom omogoča dostop do DID-dokumenta pri preverjanju veljavnosti poverilnic. Tako je shranjevanje podatkov skladno s splošno uredbo o varstvu podatkov (*angl.* General Data Protection Regulation, GDPR), saj entiteti ni treba objaviti osebnih podatkov na verigi blokov. Prvi del je identifikator sheme URI (*angl.* URI scheme identifier) »did«. V sredini se nahaja DID-metoda (*angl.* DID me-



Slika 2: **DID-arhitektura skladno s standardom W3C [19]**

thod), ki določa, kako se določena vrsta DID in z njim povezan DID-dokument ustvari, posodobi ali deaktivira. Na koncu je identifikator, specifičen za DID-metodo (*angl.* DID method specific identifier), ki ga določa DID-metoda.
did : *prism* : 6*e*368*b*3*a*7*c*42276*f* 9*ed...* (1)

- **DID URL:** enotni iskalnik virov (*angl.* Uniform Resource Locator, URL), ki razširi sintakso osnovnega DID, tako da vključi druge standardne komponente URI-ja, kot so: pot, poizvedba in fragment, da bi poiskali določen vir (primer 2).
did : *prism* : 6*e*368*b*3*a*7*c*42276*f* 9*ed.../poverilnica# diploma* (2)
- **DID-dokument (*angl.* DID document, DDO):** sestavljen iz nabora podatkov, ki opisuje DID-entitete. Do informacije pa lahko dostopajo tudi druge entitete prek DID, ki kaže nanj.
- **DID-krmilnik (*angl.* DID controller):** entiteta (oseba, organizacija ali avtonomna programska oprema), ki ima možnost, kot je opredeljeno z DID-metodo, spreminjati DID-dokument.
- **DID-entiteta (*angl.* DID subject):** glavna entiteta (oseba, skupina, organizacija, stvar ali koncept), ki jo identificira DID ter jo opiše DDO. DID-entiteta lahko pooblasti DID-krmilnik za spreminjanje DDO in je lahko hkrati tudi DID-krmilnik.
- **Preverljivi registri podatkov (*angl.* Verifiable Data Registries, VDR):** osnovni sistem ali omrežje, v katerem so DDO, DID in VC zabeleženi.

VC in VP bosta implementirana skladno s standardom W3C [20] in na verigi blokov Cardano. Kot lahko vidimo na sliki 3, bodo preverljive poverilnice vsebovale naslednje komponente: metapodatke poverilnice, kot so: vrsta poverilnice, datum izdaje in izdajatelj; eno ali več dokazil, ki je dejansko en ali več podpisov izdajatelja (vrsta, datum izdelave, nonce[1] in vrednost podpisa); enega ali več zahtevkov, ki so lahko v odvisnosti od implementacije enolični za vsak sistem, saj predstavljajo enega ali več pa-

Slika 3: **VC- in VP-struktura skladno s standardom W3C [20]**

[1] V kriptografiji je nonce poljubno število, ki se lahko uporabi samo enkrat v kriptografski komunikaciji.

rov (ključ-vrednost) podatkov o nosilcu. Preverljive predstavitve imajo podobno strukturo z majhnimi razlikami v komponentah: metapodatki v predstavitvi določajo le vrsto predstavitve in pogoje uporabe; en ali več zahtevkov iz ene ali več poverilnic skupaj z njihovimi metapodatki in dokazili so prav tako del predstavitve; podpis v VP ima enako strukturo kot podpis v VC, vendar v tem primeru podpis ustvari nosilec kot dokaz, da je on tisti, ki je izdal predstavitev preveritelju.

3 PREDLOG VPELJAVE SSI PRI PODPORI ŠTUDIJSKEGA PROCESA

Z razvojem primera uporabe, ki temelji na DID, VC in VP na verigi blokov Cardano, smo predstavili vlogo samoupravljanih identitet v študijskem procesu oziroma pri izobraževanju. Tako študentom omogočimo: upravljati s svojimi osebnimi informacijami; dokazovati svojo identiteto; hitro in preprosto uporabniško izkušnjo, ki temelji le na uporabi digitalne denarnice.

Vse tehnologije, uporabljene pri razvoju rešitve, so izbrane tako, da so čim bolj združljive z rešitvijo, ki smo jo želeli razviti. Tako smo imeli možnost sistem razviti hitreje in ga narediti učinkovejšega, varnejšega in preprostejšega za uporabnike.

3.1 Obstoječe rešitve

Za osnovo naše aplikacije smo uporabili obstoječe sisteme. Pogled na ta sorodna dela nam je pomagal razumeti, kako bomo postopali pri razvoju našega primera uporabe.

Moodle/StudIS

Moodle [11] je centralizirana platforma, ki uporabnikom omogoča komunikacijo, opravljanje nalog in spremljanje njihovih dosežkov. StudIS [14] pa je centralizirana platforma, prek katere se študentje lahko prijavijo na izpite, preverijo nekatere svoje obveznosti za tekoče leto in se prijavijo v izbrane letnike študijskih programov. Po ideji sta ti aplikaciji najbližje rešitvi, ki smo jo ustvarili, vendar s to razliko, da implementirata model centraliziranih identitet. Mi pa smo izkoristili model decentraliziranih identitet in smo uporabljali SSI na verigi blokov, kar uporabnikom ponuja popolno avtonomijo nad lastno identiteto ter hitrejši in varnejši način upravljanja z lastnimi podatki.

EduCTX

EduCTX [16] predstavlja decentralizirano platformo, ki povezuje ustanove (univerze, podjetja itn.) in njihove člane ter jim omogoča varno komunikacijo oziroma izmenjavo in preverjanje certifikatov. Ta sistem uporablja model decentraliziranih identitet na verigi blokov Ethereum [8]. Pri razvoju naše rešitve pa smo uporabili SSI na verigi blokov Cardano ter tako podprli standarda W3C za DID in VC, kar uporabnikom omogoča vzpostavitev varnejših komunikacijskih kanalov med seboj ter lažjo, hitrejšo in varnejšo izmenjavo in preverjanje poverilnic (podatkov) prek teh kanalov. Velika prednost našega sistema je tudi implementacija preverljivih predstavitev, ki uporabnikom omogočajo izbiro le tistih atributov iz svojih poverilnic, ki jih želijo deliti.

Projekt DE4A

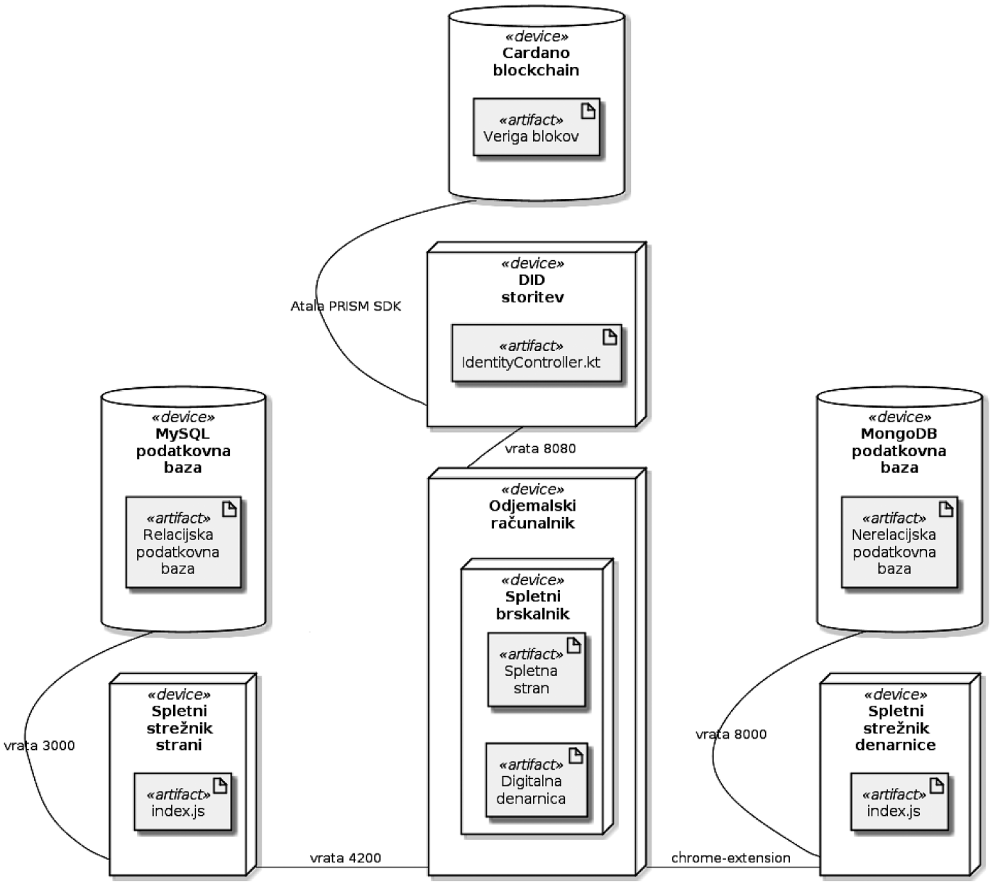
Projekt DE4A [13] vsebuje pilotne projekte različnih problemskih domen, ki temeljijo na čezmejni izmenjavi podatkov. Eden izmed njih je »Studying Abroad Pilot« [15], ki uporablja SSI oziroma DID, VC in VP za izmenjavo dokazil med posameznimi državami (univerzami), članicami EU. Primer uporabe, ki ga vključuje ter je po funkcionalnosti najbližje našemu, se imenuje »Diploma/Certs/Studies/Professional Recognition« [5] in se osredinja na priznavanje diplom, potrdil ali drugih dokazil o študiju ali tečajih. Ta primer uporabe uporablja SSI le za dokazovanje opravljenega izobraževanja, medtem ko smo obvladovanje SSI v naši rešitvi uredili za več področij, saj smo se osredinili tudi na izobraževalni proces. Z uporabo digitalne denarnice lahko študenti lažje, hitreje in varneje spremljajo svoje študijske obveznosti in potrdila v procesu študija.

3.2 Implementacija rešitve

Lastno idejo smo razvili na podlagi pregleda obstoječih rešitev in jo posodobili z uporabo SSI ter implementacijo DID, VC in VP. Glavni cilj aplikacije, ki smo jo razvili, je, da študentom ponuja naslednje možnosti: izdajo potrdil za opravljene obveznosti (izpiti, vaje, predavanja, naloge itn.), predmete; prijavo na posamezno dejavnost (izpit, kolokvij, test itn.); decentralizirano prijavo na spletni strani z uporabo DID; varno shranjevanje podatkov; preprost za uporabo in do uporabnika prijazen vmesnik; cenejšo in varnejšo uporabo verige blokov. Enkrat, ko je DID-povezava med dvema entitetama vzpostavljena (med profesorji

in študenti, med asistenti in študenti, med asistenti in profesorji, med dvema študentoma, dvema profesorjema, med študenti in delodajalci itn.), si lahko oba udeleženca v tej P2P-komunikaciji med seboj izmenjata VC in VP. Izdajatelj (profesor, asistent) v DID--komunikaciji bo nosilcu (študentu) poslal enega ali več VC, ki vsebujejo veljavne trditve o njem. Vsak VC bo podpisal izdajatelj, ki ga je izdal, kar bo omogočilo preveritelju preprosto verifikacijo veljavnosti atributov v VC. Iz ene ali več poverilnic, ki so mu bile izdane, bo lahko nosilec (študent) izbral samo potrebne atribute (podatke) in jih dodal v VP skupaj s podpisi iz vseh poverilnic, iz katerih je nosilec izbral atribute. Tako bo lahko nosilec dokazoval svojo identiteto (ime, priimek, EMŠO, datum rojstva itn.), svoje opravljene obveznosti (domače naloge, kolokvije, izpite, tečaje, programe itn.), svoj žeton dostopa do spletne strani (uporabniško ime in geslo za prijavo na spletno stran, žeton za avtentikacijo na spletni strani itn.). Preden nosilec predstavitev pošlje preveritelju (drugemu profesorju ali asistentu na isti fakulteti, drugi fakulteti ali univerzi, delodajalcu itn.), jo tudi podpiše, tako da bo lahko preveritelj preveril, ali so bili podatki v njej spremenjeni. Ko dobi VP, preveritelj preprosto prebere iz verige blokov DID nosilca in vseh izdajateljev, katerih podpisi so v VP. Tako dostopa do njihovih DID-dokumentov, da lahko prebere njihove javne ključe in preveri veljavnost vseh podpisov oziroma preveri, ali so podpisi res ustvarjeni z ustreznimi zasebnimi ključi in trenutno vrednostjo podatkov v VP. To pomeni, da mora nosilec tudi objaviti svoj DID na verigi blokov Cardano, da bi lahko ustvaril in predstavil VP preveriteljem. Glede na veljavnost podpisov in atributov se bo preveritelj odločil, ali bo nosilcu izdal poverilnico (potrdilo o opravljenem tečaju, potrdilo o opravljenem programu, potrdilo o diplomi, pogodbo o delu).

Naša rešitev je sestavljena iz različnih, medsebojno odvisnih komponent. Kot je vidno na postavitvenem diagramu (slika 4), potrebuje uporabnik na svojem računalniku le brskalnik, da lahko dostopa do spletne strani in digitalne denarnice. Ta dva sistema



Slika 4: **Postavitveni diagram**

komunicirata med seboj in z DID-storitvijo, kar uporabnikom omogoča interakcijo z lastnimi podatki.

Digitalna denarnica

Digitalna denarnica (*angl.* Digital wallet) je osrednji element in vmesnik za komunikacijo z verigo blokov. Običajno ima izbrana veriga blokov lastno denarnico, ki jo lahko uporabljajo vsi (razvijalci in uporabniki). Na žalost veriga blokov Cardano še nima digitalnih denarnic, ki bi podpirale DID, VC in VP. Zato smo ustvarili DID-storitev, ki namesto denarnice opravlja vse pomembne funkcionalnosti med entitetami. V naši rešitvi uporabljamo digitalno denarnico le kot vmesnik, ki nam prikaže, kako bi bil videti celotni sistem v praksi, če bi obstajala taka denarnica.

Razvili smo preprosto razširitev za brskalnik Chrome (*angl.* Chrome extension) z uporabo JavaScripta, CSS in HTML, ki shrani šifrirane poverilnice in podatke za generiranje javnega in zasebnega ključa v podatkovno bazo MongoDB. V praksi je shranjevanje kritičnih podatkov v centralizirani podatkovni bazi izjemno nevarno. Dejansko bi digitalna denarnica shranjevala podatke samo lokalno na napravi ali decentralizirano v obliki varnostne kopije oziroma na verigi blokov. V našem primeru poskušamo predstaviti le glavne funkcionalnosti DID, VC in VP. Poudarek torej ne bo na varnih načinih shranjevanja poverilnic in ključev pri delu z digitalno denarnico, vendar na razvoju storitve, ki bo omogočala varno in hitro izdajo, izmenjavo in potrjevanje poverilnic med entitetami pri izobraževanju.

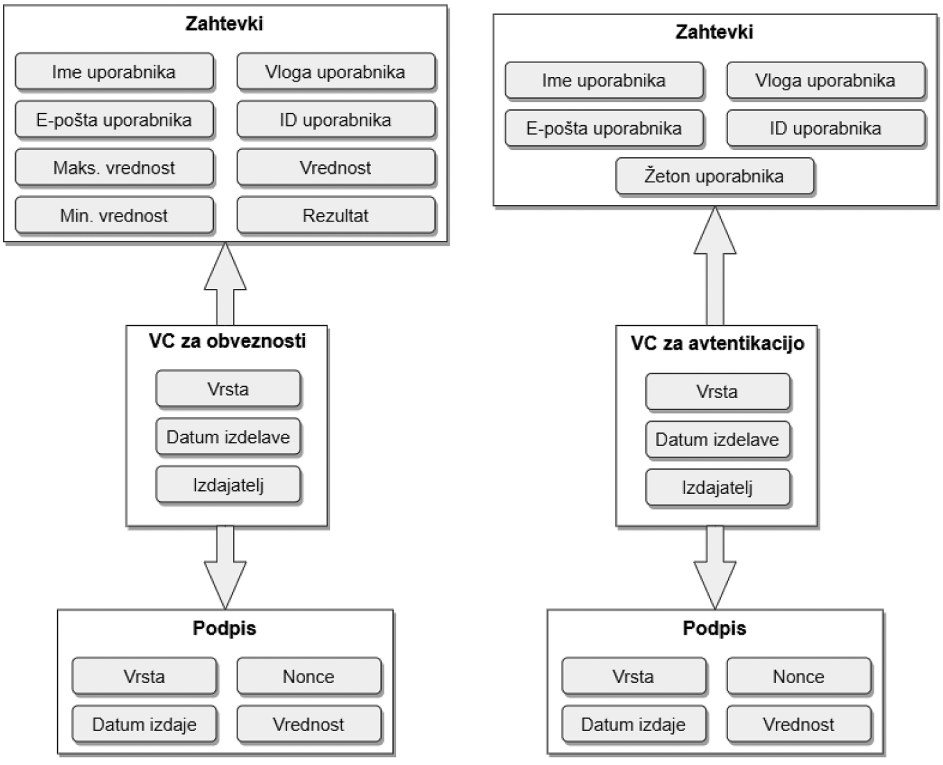
DID-storitev

Najpomembnejši del naše rešitve je DID-storitev. To je spletna storitev, ki je razvita v Kotlinu, je popolnoma decentralizirana in uporablja REST API, da bi lahko druga dva sistema komunicirala z njo. Implementira knjižnico Atala PRISM SDK [3], kar je eden izmed glavnih razlogov, zakaj smo izbrali verigo blokov Cardano, saj uporablja verigo blokov Cardano in nam omogoča cenejšo namestitev SSI ter implementacijo serije (*angl.* Batch), ki izdajateljem omogoča izdajo več poverilnic le z eno transakcijo. Atala PRISM SDK je trenutno na voljo le za razvijalce pionirskega programa Atala PRISM. Mogoče ga je preprosto implementirati v programske jezike, ki ciljajo na virtualno izvajalsko okolje Java (*angl.* Java-Virtual-Machine, JVM) in omogoča najpomembnejše funkcionalnosti skladno s standardom W3C za DID, VC in VP, kot so: generiranje, posodabljanje in preklic DID ter z njim povezan DID-dokument; objava DID na verigi blokov Cardano, kar je potrebno za poznejšo izdajo in preverjanje proverilnic; preverjanje stanja transakcije oziroma ali je transakcija uspešno objavljena na verigi blokov Cardano; branje DID-dokumenta, kar je mogoče, le če je DID že objavljen na verigi blokov Cardano; ustvarjanje, izdaja, preverjanje ter preklic poverilnice, serije in predstavitve.

Poleg implementacije velikega števila funkcionalnosti je bila ena najpomembnejših stvari določiti shemo VC v našem sistemu. Kot lahko vidimo na sliki 5, smo glede na vsebino (zahtevki) preverljive poverilnice razdelili na dve vrsti – VC za obveznosti in VC za avtentikacijo. Obe vrsti VC bosta imeli določene zahtevke enake, kot so: ime uporabnika na spletni strani, e-poštni naslov uporabnika na spletni strani, ID uporabnika na spletni strani in vloga uporabnika na spletni strani. Ti skupni atributi so v pomoč le na spletni strani, ki smo jo ustvarili v našem sistemu, da bi uporabnikom omogočili lažjo in varnejšo avtentikacijo in identifikacijo. VC za avtentikacijo je prav tako specifično za to spletno stran, saj bo vseboval tudi žeton v obliki niza, ki bo uporabniku omogočil prijavo v spletno stran s svojim DID. VC za obveznosti bo imela zahtevke, ki bodo omogočali njeno uporabo ne le na tej spletni strani: pogoj za opravljeno obveznost (maksimalna in minimalna vrednost) v numerični obliki; vrednost, ki jo je študent dosegel pri tej obveznosti v numerični obliki; rezultat v obliki niza (opravljeno ali neopravljeno). Vsi ti atributi bodo nosilcu omogočali, da s preveriteljem deli le rezultat in ali svojo oceno.

Spletna stran DIDEdu

Spletna stran DIDEdu je tudi vmesnik našega sistema, ki večinoma sodeluje z digitalno denarnico in s storitvijo DID ter ga uporabnik največ uporablja. Razvita je v Angularju (TypeScript, CSS in HTML) in uporablja podatkovno bazo MySQL za shranjevanje le najpotrebnejših podatkov o univerzah, fakultetah, uporabnikih, programih in o vsem, kar tovrstna spletna stran potrebuje za delovanje. To je aplikacija, ki omogoča uporabnikom uporabo vseh funkcionalnosti, ki jih SSI ponuja.



Slika 5: **Struktura obeh vrst preverljivih poverilnic v DID-storitvi**

Sistemu smo dodali ta centralizirani del, da bi izboljšali uporabniško izkušnjo, vendar smo razvili spletno stran na tak način, da uporabnik potrebuje svojo digitalno denarnico za uporabo funkcionalnosti spletne strani. To pomeni, da tudi če se tretja oseba prijavi prek računa nekoga drugega, ne bo mogla uporabljati funkcionalnosti spletne strani, če nima dostopa do digitalne denarnice, ki je povezana s tem računom.

4 OVREDNOTENJE

Izvorna koda rešitve je na voljo v repozitoriju Github [18], v katerem je predstavljen tudi kratek posnetek, ki prikaže delovanje najpomembnejših funkcionalnosti, ki jih rešitev implementira, kot so: DID-generiranje, preverjanje serije/poverilnice, izdaja serije/poverilnice, ustvarjanje predstavitve, preklic. Pri razvoju se nismo osredinjali na ustvarjanje aplikacije, pripravljene za produkcijsko okolje. Poudarek je bil na razvoju prototipa, ki nam pomaga predstaviti vse funkcionalnosti, ki nam jih ponuja implementacija decentraliziranih digitalnih identitet z uporabo najboljših praks in tehnologij.

V naslednjih razdelkih bomo s pomočjo SWOT-analize identificirali prednosti (*angl.* Strengths), slabosti (*angl.* Weaknesses), priložnosti (*angl.* Opportunities) in grožnje (*angl.* Threats) razvite rešitve v primerjavi s podobnimi projekti, ki smo jih že opisali v razdelku 3.1. Tako bomo povzeli splošne ugotovitve o uporabi SSI.

4.1 Prednosti

Primerjavo naše rešitve smo začeli z Moodle in s StudIS, ki sta zelo blizu naši aplikaciji, vendar obe uporabljata centraliziran model identitete. Glavne prednosti, ki smo jih ugotovili, so naslednje: naša rešitev uporablja verigo blokov, zaradi česar je gotovo varnejša; vse funkcionalnosti, ki jih ponujata oba sistema, so na voljo tudi v naši aplikaciji, kar študentom olajša dostop do njih, saj je vse potrebno pri študijskem procesu dostopno na enem mestu; ker uporabniki hranijo svoje podatke v obliki preverljivih poverilnic v lastni digitalni denarnici, centraliziranemu delu naše aplikacije ni treba hraniti toliko podatkov, kar poveča zmogljivost baze podatkov; uporabljali smo SSI, ki je vrsta decentraliziranih identitet, kar pomeni, da uporabnikom omogoča prenosljivo in ponovno uporabo lastne digitalne identitete in popolno avtonomijo nad lastnimi podatki (poverilnicami).

Nadaljujemo s primerjavo z decentraliziranim sistemom EduCTX, ki uporablja verigo blokov Ethereum: naša rešitev uporablja verigo blokov Cardano, ki je veriga blokov tretje generacije, kar pomeni, da se osredinja na stvari, kot so: razširljivost, trajnost in interoperabilnost; z implementacijo DID, VC in VP omogočimo uporabnikom varno in hitro identifikacijo, avtentikacijo in komunikacijo na spletu; implementacija Atala PRISM SDK v DID-storitvi nam omogoča hitrejšo in cenejšo namestitev SSI na verigi blokov Cardano.

Ko primerjamo naš sistem s primerom uporabe »Studying Abroad Pilot« iz projekta DE4A, ugotovimo naslednje prednosti: pri naši rešitvi ne uporabljamo DID in VC le za priznavanje opravljenega izobraževanja, ampak tudi za vse drugo, kar študenti potrebujejo v procesu študija; naš sistem implementira Atala PRISM SDK na verigi blokov Cardano, kar uporabnikom omogoča ustvarjanje serije oziroma izdajo več poverilnic z eno samo transakcijo.

4.2 Slabosti

Upoštevati moramo tudi slabosti uporabe te tehnologije. Pri primerjavi z Moodle in s StudIS ugotovimo naslednje slabosti: naša rešitev uporablja tudi verigo blokov, ki je sorazmerno nov koncept in ga ljudje še ne razumejo popolnoma ter zato ne uporabljajo decentraliziranih sistemov tako pogosto; uporabnik bo potreboval tudi digitalno denarnico in DID, da lahko izkoristi vse funkcionalnosti naše aplikacije.

Pri primerjavi naše rešitve z EduCTX ugotovimo, da Ethereum omogoča druge funkcionalnosti, zaradi katerih je veriga blokov Cardano lahko slabša; veriga blokov Cardano je še vedno v razvoju oziroma še vedno razvija nekatere funkcionalnosti, ki jih je Ethereum že razvil pred nekaj leti.

Slabosti, ki smo jih našli pri primerjavi naše rešitve s projektom DE4A, so naslednje: naša rešitev prikazuje DID v njihovi normalni obliki, kar ni dobra praksa, saj jih uporabnik ne more preprosto prebrati in uporabljati; kot smo že omenili v razdelku 3.2, veriga blokov Cardano še nima razvite delujoče digitalne denarnice, ki bi podpirala DID, VC in VP; ustvariti smo jo morali sami z uporabo centralizirane podatkovne baze MongoDB za shranjevanje šifriranih poverilnic, kar se v praksi ne bi zgodilo, saj omejuje nadzor uporabnika nad lastnimi podatki.

4.3 Priložnosti

Na splošno so priložnosti, za katere smo ugotovili, da prihajajo z uporabo samoupravljanih identitet na verigi blokov ter pri izobraževanju, naslednje: uporaba verige blokov namesto baze podatkov ni samo varnejša, ampak tudi boljša v smislu zmogljivosti, saj več kot je objavljenih blokov (podatkov), varnejša postane veriga blokov; uporaba DID, VC in VP v več aplikacijah poveča zanimanje razvijalcev in uporabnikov za razvoj in uporabo decentraliziranih sistemov, ki podpirajo SSI; uporaba SSI pri izobraževanju študentom omogoča lažji dostop in dokazovanje svojih izobraževalnih dosežkov do storitev v celotnem študijskem ekosistemu in širše; več implementacij SSI na spletu uporabnikom omogoča lažjo in širšo uporabo SSI ter varno, prenosljivo in ponovno uporabo lastnih podatkov v vsakem sistemu, v katerem so te tehnologije implementirane.

4.4 Grožnje

Obstaja tudi nekaj groženj pri uporabi SSI na verigi blokov in pri izobraževanju: uporabniki imajo večjo odgovornost za varnost svojih podatkov, saj so vse njihove poverilnice šifrirane in shranjene na njihovih osebnih napravah (digitalnih denarnicah); izguba ali deljenje zasebnega ključa oziroma dostopa do denarnice uporabnika prek tretjih oseb omogoča zlonamernim entitetam dostop do osebnih podatkov in kriptovalut lastnika; DID, VC in VP se začnejo uvažati v druge verige blokov, ki imajo mogoče večjo sprejetost uporabnikov kot Cardano, kar lahko povzroči, da razvijalci izberejo drugo verigo blokov; zaradi avtomatizacije številnih procesov s pomočjo SSI pri izobraževanju se bo brezposelnost povečala; Atala PRISM SDK uporablja testno omrežje verige blokov Cardano, kar lahko povzroči, da je naš sistem nestabilen pri funkcionalnostih, ki uporabljajo verigo blokov.

5 SKLEP

Decentralizirana aplikacija, ki smo jo razvili za izobraževalne institucije, študentom omogoča lažje, hitrejše in varnejše spremljanje svojih študijskih obveznosti ter potrdil. Razvoj te rešitve nam je pomagal predstaviti obvladovanje vrste modela decentraliziranih identitet, ki podpira DID, VC in VP pri izobraževanju. Vpeljava SSI na verigo blokov Cardano upo-

rabnikom omogoča: prenosljivost, varno in ponovno uporabo podatkov na spletu; uporabo Atala PRISM SDK oziroma implementacijo DID, VC in VP skladno s standardom W3C ter cenejšo namestitev SSI na verigi blokov; popoln nadzor nad lastnimi podatki. S pomočjo testiranja in SWOT-analize smo ugotovili, da je ta decentraliziran sistem dejansko hitrejši, varnejši in primernejši za študente kot nekatere že obstoječe rešitve. Seveda obstajajo nekatere slabosti, ki prihajajo z uporabo te tehnologije na verigi blokov Cardano, kot so: manjkajoča digitalna denarnica za delo z DID, VC in VP; funkcionalnosti, ki so še vedno v razvoju; uporaba testnega omrežja verige blokov Cardano; težko razumevanje tehnologije verige blokov pri uporabnikih in razvijalcih; večja odgovornost entitet za varnost njihovih osebnih podatkov.

Pokazali smo, da imajo samoupravljane identitete pomembno vlogo pri izobraževanju, vendar jih je vredno uporabiti v čim več ter različnih primerih uporabe. Decentralizacija ter s tem popolna avtonomija in varnost digitalnih identitet se morajo nenehno nadgrajevati, zato pa moramo zbuditi zanimanje več razvijalcev v razvoj decentraliziranih rešitev z uporabo te tehnologije. Več primerov uporabe kot povežemo z njo, večjo prenosljivost in več nadzora nad večjim številom lastnih podatkov bodo imeli uporabniki.

Če bi bila vsaka rešitev decentralizirana in bi uporabljala SSI oziroma DID, VC in VP kot način za izmenjavo, preverjanje in shranjevanje osebnih podatkov s pomočjo verige blokov, bi uporabniki potrebovali le svojo denarnico, da bi lahko varno in hitro delali z lastnimi podatki, kot želijo in kadar želijo. Tako se bo začela nova doba spleta, v kateri bo internet tisto, kar naj bi vedno bil – varno mesto, ki ljudem lajša življenje brez nevarnosti zlorabe njihovih podatkov.

LITERATURA

[1] Aggarwal, S., & Kumar, N. (2021). Chapter Sixteen – Hyperledger Working model. V S. Aggarwal, N. Kumar & P. Raj (Ur.), *The Blockchain Technology for Secure and Smart Applications across Industry Verticals* (str. 323–343). Elsevier. https://doi.org/https://doi.org/10.1016/bs.adcom.2020.08.016

[2] Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017). Blockchain technology innovations. *2017 IEEE Technology and Engineering Management Conference (TEMSCON)*, 137–141. https://doi.org/10.1109/TEMSCON.2017.7998367

[3] *Atala PRISM SDK*. (2022). Pridobljeno 26. septembra 2022, https://docs-ppp.atalaprism.io/

[4] Camp, J. (2004). Digital identity. *IEEE Technology and Society Magazine, 23*(3), 34–41. https://doi. org/10.1109/MTAS.2004.1337889

[5] *Use Case "Diploma/Certs/Studies/Professional Recognition" (SA UC3)*. (2022). Pridobljeno 26. septembra 2022, https://wiki.de4a.eu/index.php/Use_Case_%22Diploma/Certs/Studies/Professional_ Recognition%22_(SA_UC3)

[6] Fang, J., Yan, C., & Yan, C. (2009). Centralized Identity Authentication Research Based on Management Application Platform. *2009 First International Conference on Information Science and Engineering*, 2292–2295. https://doi.org/10.1109/ICISE.2009.382

[7] Isirova, K., & Potii, O. (2018). Decentralized public key infrastructure development principles. *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DES-SERT)*, 305–310. https://doi.org/10.1109/DESSERT.2018.8409149

[8] Kushwaha, S. S., Joshi, S., Singh, D., Kaur, M., & Lee, H.-N. (2022). Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract. *IEEE Access, 10*, 6605–6621. https://doi.org/ 10.1109/ACCESS.2021.3140091

[9] Laurent, M., & Bouzefrane, S. (2015). *Digital identity management*. Elsevier.

[10] *The Three Models of Digital Identity Relationships*. (2018). Pridobljeno 5. novembra 2022, https://medium.com/evernym/the-three-models-of-digital-identity-relationships-ca0727cb5186

[11] *Moodle documentation*. (2022). Pridobljeno 26. septembra 2022, https://docs.moodle.org/400/en/ Main_page

[12] Preukschat, A., & Reed, D. (2021). *Self-Sovereign Identity.* Manning.

[13] *DE4A Service Interoperability Solutions Toolbox)*. (2022). Pridobljeno 26. septembra 2022, https://wiki.de4a.eu/index.php/DE4A_Service_Interoperability_Solutions_Toolbox

[14] *StudIS FRI*. (2022). Pridobljeno 5. oktobra 2022, https://studisfri.uni-lj.si/Account/Login?ReturnUrl=%2f

[15] *Studying Abroad Pilot*. (2022). Pridobljeno 26. septembra 2022, https://wiki.de4a.eu/index.php/ Studying_Abroad_Pilot

[16] Turkanovic´, M., Hölbl, M., Košič, K., Heričko, M., & Kamišalic´, A. (2018). EduCTX: A Blockchain- Based Higher Education Credit Platform. *IEEE Access, 6*, 5112–5127. https://doi.org/10.1109/ ACCESS.2018.2789929

[17] van Bokkem, D., Hageman, R., Koning, G., Nguyen, L., & Zarin, N. (2019). Self-Sovereign Identity Solutions: The Necessity of Blockchain Technology. https://doi.org/10.48550/ARXIV.1904.12816

[18] Vasilev, N. (2022). *DIDEdu-DiplomskoDelo* (Ver. 2.0.4). Pridobljeno 26. septembra 2022, https : //github.com/nikolayVv/DIDEdu

[19] *Decentralized Identifiers (DIDs) v1.0.* (2021). Pridobljeno 26. septembra 2022, https://www.w3.org/ TR/did-core/

[20] *Verifiable Credentials Data Model v1.1*. (2022). Pridobljeno 26. septembra 2022, https://www.w3.org/ TR/vc-data-model/

[21] *W3C Standards.* (b.d.). Pridobljeno 22. septembra 2021, https://www.w3.org/standards/

[22] Yan, L., Rong, C., & Zhao, G. (2009). Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based Cryptography. V M. G. Jaatun, G. Zhao & C. Rong (Ur.), *Cloud Computing* (str. 167–177). Springer Berlin Heidelberg.

▪

Nikolay Vasilev je diplomiral leta 2022 na fakulteti za računalništvo in informatiko Univerze v Ljubljani. Njegova raziskalna zanimanja vključujejo decentralizirane sisteme, varnost, biometrijo in decentralizirane identitete.

▪

Dejan Lavbič je izredni profesor na fakulteti za računalništvo in informatiko Univerze v Ljubljani. Njegova raziskovalna področja so: kakovost informacij, semantični splet, Splet3, decentralizirane verige blokov in decentralizirane identitete. Sodeloval je v številnih EU- in nacionalni projektih ter ima dolgo zgodovino sodelovanja z gospodarstvom..