Specifikacija arhitekture samoupravljivog identiteta (SSI)

Šeila Bećirović
Elektrotehnički fakultet Sarajevo)
Univerzitet u Sarajevu
Sarajevo, Bosna i Hercegovina
sbecirovic1@etf.unsa.ba

Saša Mrdović
Elektrotehnički fakultet Sarajevo)
Univerzitet u Sarajevu
Sarajevo, Bosna i Hercegovina
smrdovic@etf.unsa.ba

***Sažetak*—Razvoj blockchaina omogućio je razvoj novih koncepata i ideja. Jedan od njih je samoupravljivi identitet (engl. Self-sovereign identity - SSI). Cilj ovog rada je analizirati različite arhitekture SSI-a izvedene primjenom blockchain tehnologija. Definisani su i objašnjeni gradivni koncepti SSI-a, kao i različite arhitekture te potencijalni problemi koji mogu nastati primjenom različitih arhitektura, te su definisana otvorena pitanja za dalji rad.**

Ključne riječi: Blockchain, samoupravljivi identitet, arhitektura SSI

I. Uvod

Potpuna kontrola nad vlastitim digitalnim identitetom je pristup koji svakim danom postiže sve veću privlačnost. Danas, ovaj koncept pronalazimo u modelu upravljanja identitetom poznatom kao samoupravljivi identitet. Samoupravljivi identitet je model upravljanja identitetom, gdje je korisnik vlasnik podataka i kontroliše i upravlja identitetom i svim pripadajućim podacima [1]. Svaki korisnik može slobodno kontrolirati i manipulirati svojim digitalnim identitetom, uključujući lične podatke, primati i prikupljati provjerljive potvrde od izdavatelja i birati koje informacije želi dijeliti bez oslanjanja na bilo koje vanjsko ovlaštenje. Infrastruktura za upravljanje identitetom je donekle decentralizovana i to eliminiše jednu tačku neuspjeha i povećava sigurnost, povjerenje i privatnost. Smatra se da je samosuvereni identitet još u začetku, te postoji samo nekoliko standarda i arhitektura koje ga u potpunosti definiraju [2]. Razvoj SSI-ja je započet razvojem decentralizirane tehnologije, konkretno blockchain tehnologije, iako ista nije uvijek potrebna za implementaciju SSI [3].

Blockchain je javna ili privatna distribuirana baza podataka izgrađena na peer-to-peer mreži [4]. Omogućava sporazume o transakcijskim podacima, dijeljenje podataka preko mreže nepouzdanih učesnika, bez oslanjanja na centralni pouzdani autoritet. Blockchain klijenti koji rade na blockchain mrežnim čvorovima verificiraju i pohranjuju transakcije u kontinuiranu bazu, odnosno u glavnu knjigu (eng. ledger), u koju se samo dodaju transakcije. Da bi se postiglo povjerenje, većina čvorova mora postići konsenzus o stanju transakcijskih podataka. Struktura podataka blockchaina je lista blokova, koji se mogu identificirati, koji pohranjuju unaprijed definirani maksimalni broj transakcija i kriptografski su povezani s prethodnim blokom. Blokovi formiraju lanac [5]. Tehnologije distribuirane knjige (DLT) kao što je Blockchain mogu se koristiti kao dio ekosistema za SSI.

U ovom radu fokusiramo se na vezu između blockchain tehnologije i SSI. Cilj ovog rada je uvesti arhitektonske pristupe i obrasce za SSI na blockchain-u. U odjeljku II predstavljeno je trenutno stanje tehnike. U odjeljcima III i IV dati su građevinski blokovi SSI i arhitektonski pristupi. Kroz pregled arhitekture i vodećih procesa u postojećim SSI-a, u završnom dijelu će se donijeti zaključak i dati prijedlog za buduća istraživanja.

II. Povezani radovi

Budući da je SSI tehnologija u nastajanju, istraživanje se provodi u definiranju njegovih procesa, komponenti i arhitekture.

Muehle i dr. u [6] su dali pregled samoupravljivog identiteta. Oni daju jednostavnu definiciju arhitekture u kojoj identifikuju i detaljno objašnjavaju četiri glavne komponente SSI: identifikacija (DID), autentikacija (DLT), provjerljive potvrde (VC) i skladištenje.

U [7], autori predlažu različite obrasce za aplikacije zasnovane na blockchain-u. Među njima, oni uvode obrazac reverse-oracle koji se može koristiti za decentralizirane identitete.

Toth i Priddy predstavljaju jedno od najranijih rješenja SSI arhitekture u svom radu [8]. Oni definiraju komponente, glavne funkcije i karakteristike, a sve to ugrađujući SSI kao sloj povjerenja u različite aplikacije.

Lim i dr. su u radu [9] uradili pregled i analizu 15 aplikacija. Aplikacije su ili profitne ili neprofitne, vezane za vlade, razvile su ih kompanije ili su open-source rješenja. Oni su došli do zaključka da je SSI optimalno rješenje za korisnički-orijentisan, siguran i troškovno-efektivan IAM.

U radu [10] izvršen je pregled šest SSI sistema, identificirana su potencijalna poboljšanja na istim.

Gilani i dr. [11] su izvršili pregled osam SSI rješenja. Naglasili su one koji podržavaju selektivno otkrivanje, identificirali su načine čuvanja kritpografskih ključeva, te detalje o DLT-u.

U radu [12] opisano je deset SSI sistema. Svaki sistem je analiziran u sklopu 10 principa SSI-a i provjereno je da li zadovoljavaju iste.

U [13], autori prikupljaju, definiraju i predlažu 12 različitih dizajnerskih obrazaca za SSI izgrađen na blockchainu. Svrha ovih obrazaca je da pomognu arhitektima da razumiju i lako primjene koncepte u dizajnu sistema. Oni su kategorizirali obrasce u tri kategorije: ključni obrasci upravljanja, decentralizirani obrasci upravljanja identifikatorima i obrasci dizajna potvrda.

.

III. Principi, taksonomija i osnovni gradivni blokovi SSI-a

A. Principi SSI

SSI dozvoljava ljudima da vrše interakcije u digitalnom svijetu na isti način kao i u "offline" svijetu. Samim tim, Cristopher Allen je definisao deset principa koje SSI mora zadovoljavati [14]:

1) Pristup (eng. Access) - Korisnici moraju imati pristup svojim podacima.
2) Saglasnost (eng. Consent) - Korisnici se moraju složiti s potencijalnom upotrebom njihovog identiteta.
3) Kontrola (eng. Control) - Korisnici kontrolišu svoj identitet.
4) Postojanost (eng. Existence) - Korisnici imaju neovisno postojanje.
5) Interoperabilnost (eng. Interoperability) - Identiteti se mogu maksimalno koristiti.
6) Minimalizacija (eng. Minimalization) - Informacije na potvrdama su minimizirane.
7) Perzistentnost (eng. Persistence) - Identiteti moraju dugo živjeti.
8) Zaštita (eng. Protection) - Prava korisnika se moraju zaštititi.
9) Portabilnost (eng. Portability) - Informacije i usluge vezane za identitet se moraju moći prenositi.
10) Transparentnost (eng. Transparency) - Sistemi i algoritmi su opće poznati.

Postizanje osnova ovih principa se postiže korištenjem odgovarajućih gradivnih elemenata SSI. Da bi razumjeli SSI, potrebno je objasniti SSI elemente. U nastavku je dato objašnjenje osnovnih pojmova vezanih za SSI.

B. Taksonomija SSI

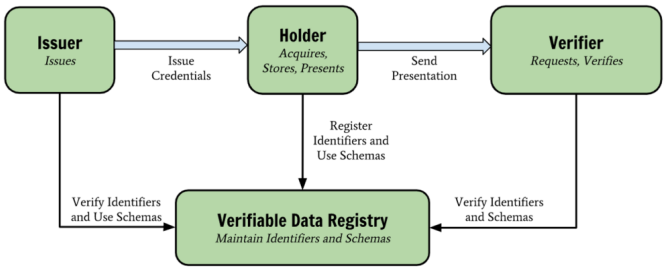
Osnovni pojmovi vezani za SSI su:

1) Atribut (eng. Attribute) - Karakteristika subjekta [15];
2) Autentikacija (eng. Authentication)- Proces kojim korisnik dokazuje da posjeduje token, privatni ključ ili biometrijske informacije, koje samo on može posjedovati i na taj način se identificira. [16].
3) Decentralizovana knjiga (eng. Decentralized ledger) - Necentralizovan sistem za spašavanje transakcija. Ovi sistemi uspostavljaju dovoljno povjerenja, te se učesnici mogu osloniti na podatke koje su drugi zabilježili. Obično koriste distribuirane baze podataka u kojima različiti čvorovi koriste protokol konsenzusa za potvrdu redoslijeda kriptografski potpisanih transakcija. Povezivanje digitalno potpisanih transakcija tokom vremena često čini historiju knjige praktično nepromenljivom [16].Pomoću DLT-a je omogućeno da svi u mreži imaju isti izvor istine, i u isti se pohranjuju hash-evi DID-ova ili javni ključevi. DLT predstavlja provjerljivi registar podataka. Nadalje, u nekim vladinim okvirima poput Evropskog SSI okvira (ESSIF), DLT-ovi se koriste za različite registre, npr. registar pouzdanih izdavatelja, DID registar itd. [17]. Koristeći blockchain, SSI entiteti koji učestvuju (nosioci identiteta, izdavaoci i verifikatori) mogu dodatno provjeriti nečiji identitet i potvrde. Strane koje provjeravaju, osim provjere valjanosti podataka u dokazu (tj. provjerljive prezentacije), koriste blockchain za dodatnu provjeru valjanosti podataka prezentacije (npr. atest i strana koja potvrđuje) provjeravanjem identiteta izdavaoca i/ili valjanosti potvrde (npr. liste opoziva) itd.
4) Decentralizovani identifikator (eng. Decentralized Identifier - DID) - W3C definira decentralizirane identifikatore (DID) kao "novi tip identifikatora koji omogućava provjerljiv, decentralizirani digitalni identitet. DID se odnosi na bilo koji subjekt (npr. osobu, organizaciju, stvar, model podataka, apstraktni entitet, itd.) koji je odredio kontroler DID-a. Za razliku od tipičnih, federalnih identifikatora, DID-ovi su dizajnirani tako da mogu biti odvojeni od centraliziranih registara, dobavljača identiteta i tijela za izdavanje certifikata. " DID-ovi su URI-ji koji povezuju DID subjekt sa DID dokumentom omogućavajući pouzdane interakcije povezane s tim subjektom [16].
5) Delegat (eng. Delegate) - Entitet čijim identitetom upravlja staratelj [16].
6) Dokument decentralizovanog identifikatora (eng. DID document) - DID dokument predstavlja skup podataka koji opisuju DID subjekt, uključujući mehanizme, kao što su kriptografski javni ključevi, koje DID subjekt ili DID delegat može koristiti da se autentifikuje i dokaže svoju povezanost sa DID-om.
7) Entitet (eng. Entity) - Osoba, organizacija ili stvar [18]
8) Graf (eng. Graph) - Mreža informacija sastavljena od subjekata i njihovog odnosa prema drugim subjektima ili podacima [19].
9) Identifikatori (eng. Identifier) - Atribut ili set atributa koji jedinstveno opisuju identitet. [15]
10) Identitet (eng. Identity) - Skup atributa jednog entiteta [15].
11) Izdavač (eng. Issuer) - Entitet koji izdaje potvrde o subjektu na zahtjev [18].
12) Izvedeni predikat (eng. Derived predicate) - Provjerljiva, logička tvrdnja o vrijednosti drugog atributa u provjerljivim potvrdama [19].
13) Korisnički agent (eng. User agent) - Program kao što je preglednik, koji vrši medijaciju između vlasnika,

izdavača i verifikatora [20].

14) Minimizacija podataka (end. Data minimization) - Svođenje dijeljenjih podataka na minimum potreban za postizanje cilja [19].
15) Druga stranka (eng. Relying party) - Entitet koji dobije informacije o subjektu od verifikatora [18].
16) Potvrda (eng. Credential) - Skup tvrdnji koje izdaje izdavač [19].
17) Prezentacija (eng. Presentation) - Informacija dobijena kroz jednu ili više potvrda, koju subjekt otkriva verifikatoru o sebi [18]
18) Prezenter (eng. Presenter) - Entitet koji pruža informacije kroz prezentaciju [19].
19) Provjerljiva prezentacija (eng. Verifiable presentation) - Prezentacija na kojoj se vide neovlašetena mijenjanja i koja je enkodirana na način da se može vjerovati autorstvu nakon procesa kriptografske provjere [19].
20) Provjerljive potvrde(eng. Verifiable credentials - VC) - standardni model podataka i format predstavljanja kriptografski provjerljivih digitalnih potvrda [16]. VC predstavlja potvrdu na kojoj se vidi neovlašteno mijenjanje i čije se autorstvo može kriptografski verificirati [19]
21) Pružatelj identiteta (eng. Identity provider - IdP) - Sistem zadužen za kreiranje, održavanje i upravljanje informacijama o identitetu [19] za vlasnike identiteta.
22) Repozitorij (eng. Repository) - Program ili digitalni novčanik u kojem se čuvaju provjerljive potvrde [19].
23) Selektivno otrkivanje (eng. Selective disclosure) - Mogućnost subjekta da bira šta će otkriti [19].
24) Staratelj (eng. Custodian) - Entitet koji može da predstavlja drugi entitet i koristi njegov identitet i potvrde [18].
25) Subjekat (eng. Subject) - Entitet koji prima jednu ili više potvrda od izdavača [18].
26) Tvrdnja (eng. Claim) - Karakteristika subjekta koju opisuje izdavač u sklopu provjerljive potvrde [18].
27) URI (eng. Uniform Resource Identifier) - Standardni format identifikatora za sve resurse na Internetu. DID je tip URI sheme [16].
28) UUID (eng. Universally Unique Identifier) - Tip globalno jedinstvenog identifikatora. Sličan je DID jer ne treba centralni autoritet, ali nije kriptografski provjerljiv [16].
29) Validacija (eng. Validation) - Proces provjere da li provjerljiva prezentacija ili potvrda zadovoljavaju određen uslove verifikatora [19].
30) Verifikacija (eng. Verification) - Proces određivanja da li su informacije vezane za određeni identitet [15].
31) Verifikator (eng. Verifier) - Entitet koji verificira validnost prezentacije za druge stranke [18].
32) Vlasnik identiteta (eng. Holder) - Uloga entiteta koji posjeduje provjerljive potvrde i koji vrši prezentovanje istih [18].
33) Vlasnik sistema (eng. System owner) - Vlasnik sistema za upravljanje identitetom [18].
34) Zahtjevatelj (eng. Requester) - Entitet koji zahtjeva od izdavača određenu potvrdu o subjektu [18]. Posjednik identiteta, subjekat i zahtjevatelj mogu biti jedan entitet.

Grafički prikaz SSI tôka i određenih elemenata je dat na slici 1



Slika 1. SSI tôk [16]

C. Osnovni scenarij upotrebe SSI-a

Ideja SSI-a da živimo u svijetu bez papira i potvrda, odnosno dokazivanja identiteta kroz pisani trag i ovjereni dokument je jedan od glavnih razloga za daljni razvoj istog. Osnovni scenarij upotrebe SSI podrazumijeva korištenje SSI infrastrukture za dobivanje digitalnih dokumenata i dokazivanje istih. Na slici 2 je prikazan jedan scenarij, čiji su koraci objašnjeni u nastavku:

1) Korisnik dobiva digitalnu diplomu u obliku VC-a od univerziteta. Istu smješta u svoj digitalni novčanik. Univerzitet na blockchain smješta kriptografske dokaze izdavanja diplome.
2) Prilikom prijave za posao on budućem poslodavcu šalje svoju digitalnu diplomu.
3) Poslodavac na blockchain-u provjera kriptografski dokaz diploma i potvrđuje njenu validnost.
4) Poslodavac prihvata digitalnu diplomu korisnika.

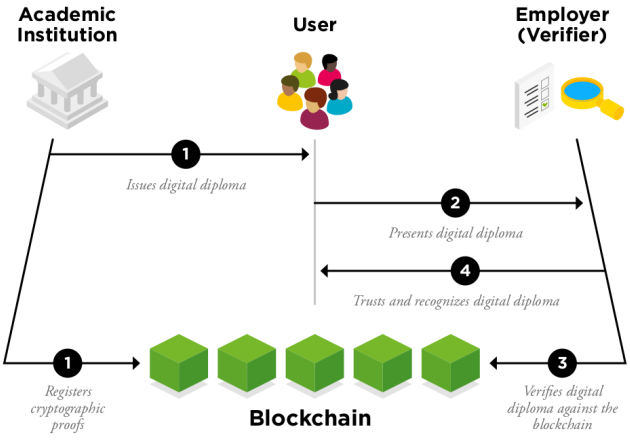
Razlike između ovog scenarija i današnjeg standardnog se ogledaju u činjenici da prilikom procesa provjere diplome, poslodavac mora direktno kontaktirati akademsku instituciju, dok u SSI je sve provjerljivo kroz DLT. [20]

IV. Arhitektura SSI

Definisanje kompletne arhitekture SSI nije jednostavan zadatak. Od rane definicije SSI, bilo je nekoliko predloženih rješenja i implementacija SSI. Ova različita rješenja uključuju različite arhitekture i novo-definirane nestandardizirane koncepte. Osnovne komponente i njihovi odnosi prisutni su u svakoj predloženoj arhitekturi.

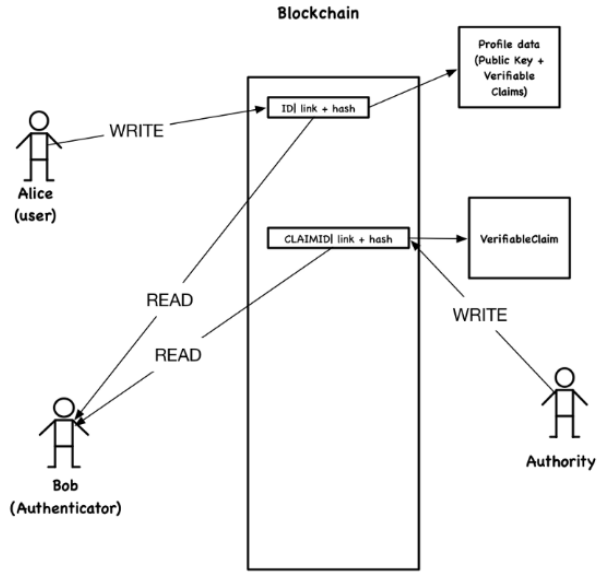
A. Upravljanje identitetom i pristupom (IAM) koristeći blockchain

U članku [21], autor predstavlja obrazac arhitekture za upravljanje identitetom i pristupom (eng. Identity Access and Management - IAM) koristeći blockchain. Na ovaj prijedlog možemo gledati kao na prethodnicu za SSI. Potreba za



Slika 2. Slučaj upotrebe [20]

decentralizovanim IAM okruženjem proizilazi iz želje da se spreči da jedan lažni korisnik ili nekoliko korisnika značajno utiču na sistem. Predloženo rješenje je bazirano na W3C specifikacijama VC-a i DID-a kao što je dato na slici 3.

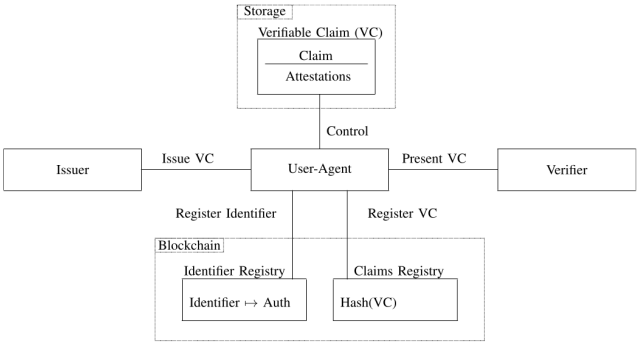


Slika 3. Uzorak IAM arhitekture zasnovan na blokčejnu [21]

Ideja arhitekture je da osoba,npr. Alice kreira identitet (DID) i sa njim se upisuje u blockchain. Ovaj upis uključuje nasumično generirani identifikator, vezu do aplikacije sa identifikatorima i hash podatake profila. Korisnički profil sadrži javni ključ i skup provjerljivih tvrdnji. Generirani nasumični identifikator sada postaje njen DID, jer samo ona posjeduje privatni ključ koji odgovara javnom ključu. Provjerljive tvrdnje su tokeni delegiranja potpisani od strane nadležnog organa. Kreator ih također snima u blockchain zajedno sa hashom zahtjeva na način sličan DID-u. Alice dolazi do provjerljivih tvrdnji prije svega odlaskom vlastima. Na primjer, matični ured je odgovarajući autoritet za provjerljive tvrdnje imena, adrese i datuma rođenja. Pod pretpostavkom da vlasti izdaju provjerljive tvrdnje, Alice prvo demonstrira svoje vlasništvo nad DID-om korištenjem protokola izazov-odgovor. Zatim podnosi zahtjeve za provjerljive potvrde za svoje atribute, koji mogu, na primjer, uključivati njeno ime, adresu, diplomu i datum rođenja. Kako bi ažurirala podatke svog profila, Alice će dodati novi unos u blockchain s novim hash profila. U protokolu izazov-odgovor, validator generiše nasumičnu vrijednost, šifrira je koristeći javni ključ, a zatim izaziva Alice da pokaže da ima privatni ključ dešifrovanjem šifrovane vrijednosti. Pošto Alice ima privatni ključ, ona mora biti vlasnica DID-a. Drugi korisnik ili organizacija (autentifikator), Bob, koji želi identificirati Alice, prvo prima DID od Alice, čita sve unose koji se odnose na taj DID iz blockchaina, dohvata podatke o Alice-inom profilu i provjerava ih. Bob može potvrditi njen identitet koristeći protokol izazov-odgovor. Tako Bob može potvrditi provjerljive tvrdnje i biti siguran da su tvrdnje o Alice istinite. Osnova ovog arhitektonskog obrasca protkana je kroz čitavu diskusiju o arhitekturi SSI-a [21].

B. Model registra identifikatora

Jedna od prvih definicija SSI arhitekture data je u [6]. SSI model je usmjeren na korisnika, za razliku od prethodnih modela identiteta gdje je centar pružatelj usluga. Osnova SSI je distribuirana knjiga (blockchain ili druga). DLT služi kao zamjena za autoritet za registraciju i funkcioniše kao registar identifikatora. Koristeći ga, identifikacija i autentifikacija se održavaju putem kriptografskih protokola. DID i VC se pohranjuju u aplikaciju koju kontrolira korisnik (novčanik) i koja je obično izvan lanca kako bi se očuvala privatnost. Ovaj model je poznat kao model registra identifikatora i prikazan je na slici 4. Proširenje ovog modela poznato je kao model registra tvrdnji gdje blockchain ne funkcionira samo kao registar za identifikatore, već također drži kriptografske dokaze svih povezanih tvrdnji.



Slika 4. Model registra identifikatora [6]

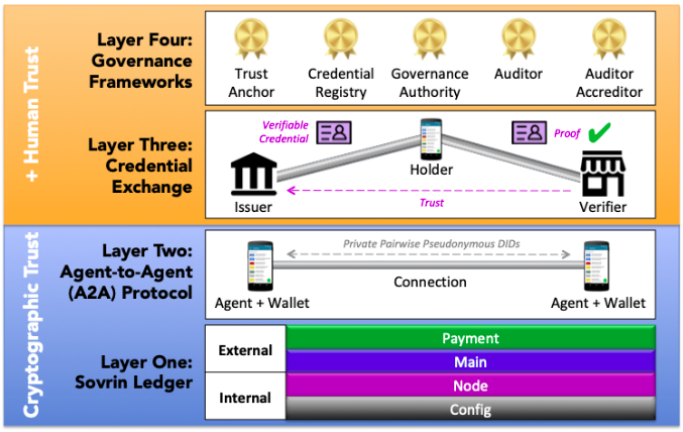
Proširenja ove jednostavne arhitekture mogu se naći u rješenjima kao što su Sovrin, Everynm, ShoCard, uPort i druga.

C. Sovrin stek

Sovrin je predstavio četveroslojni infrastrukturni model pod nazivom Sovrin Stack. Grafički prikaz steka je prikazan na

slici 5 Četiri sloja su [22]:

1) Sovrin sloj distribuirane glavne knjige (eng. Sovrin Ledge Layer) - donji sloj i osnova javnih Sovrin identiteta ukorijenjenih u Anywise DID-ovima. Ova knjiga uključuje sheme, definicije potvrda i registre opoziva.
2) Protokol agent ka agentu (Agent-to-Agent - A2A) - ključno je za Sovrin entitete da formiraju veze, održavaju novčanike i razmjenjuju potvrde preko direktnih peer-to-peer veza bez upotrebe DLT-a.
3) Sloj razmjene potvrda (eng. Credential Exchange Layer) - prva dva sloja uspostavljaju kriptografsko povjerenje (eng. Cryptographic Trust), ali ne uspostavljaju ljudsko povjerenje (eng. Human trust). U ovom sloju izdavači izdaju potvrde vlasnicima. Vlasnici se ponašaju kao dokazivači i verifikatorima predstavljaju dokaze ovih potvrda. Verifikatori koriste prvi sloj kako bi provjerili DID izdavača, odnosno kako bi preuzeli javni ključ i na osnovu njega provjerili taj dokaz.
4) Sloj okvira upravljanja (eng. Governance Framework Layer)– Neke potvrde su vrlo uskog opsega – izdaje ih jedan izdavač. Postoje potvrde koje su namijenjene širem usvajanju (izvod iz matične knjige rođenih, pasoši, vozačke dozvole) i obično imaju više izdavača i bilo koji broj verifikatora. Ljudsko povjerenje se zasniva na grupi organizacija kao što su banke, prodavnice, pružaoci zdravstvenih usluga, univerziteti i vlade. Da bi se osiguralo ljudsko povjerenje, definisani su okviri upravljanja.

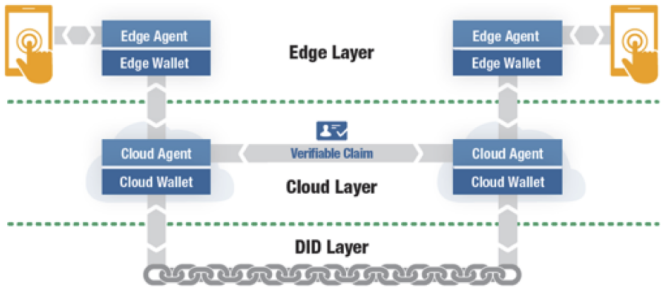


Slika 5. Sovrin Stack [22]

D. Evernym

Everynm isto tako uvodi slojevitu arhitekturu. Oni definiraju SSI stack sa Decentralized Key Management System - DKMS (otvoreni standard za upravljanje korisničkim DID-ovima i privatnim ključevima) datim na slici 6 sa sljedećim slojevima [23]:

1) DID sloj (eng. DID Layer) je temeljni sloj koji se sastoji od DID-ova registrovanih i provjerljivih preko DLT-a.
2) Sloj oblaka (eng. Cloud Layer) se sastoji od agenata na strani servera i novčanika koji pružaju sredstva za komunikaciju i posredovanje između DID sloja i rubnog sloja. Ovaj sloj omogućava šifrovanu peer-to-peer komunikaciju za razmjenu i verifikaciju DID-ova, javnih ključeva i potvrda koje se mogu provjeriti.
3) Rubni sloj (eng. Edge Layer) se sastoji od lokalnih uređaja, agenata i novčanika koje direktno koriste vlasnici identiteta za generiranje i pohranjivanje većine privatnih ključeva i izvođenja većine operacija upravljanja ključevima.



Slika 6. Everynm SSI Stack [24]

E. uPort

UPort arhitektura uključuje tri glavna elementa [25]:

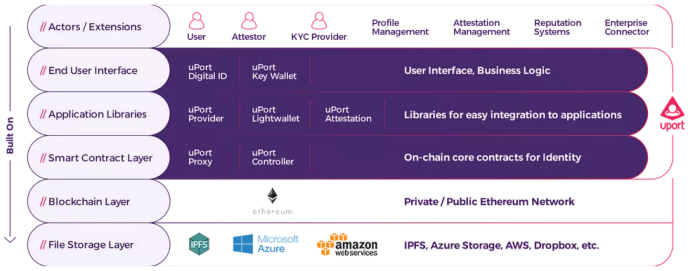
- Pametni ugovori (eng. Smart contracts) koji potvrđuju identitet korisnika i sadrže logiku koja omogućava korisniku da povrati svoj identitet ako izgubi mobilni uređaj.
- Mobilna aplikacija u sklopu koje se nalaze ključevi korisnika i koja omogućava njegovu komunikaciju sa pametnim ugovorom (potpisivanje transakcije). Ključ se čuva hardverski kroz sigurnu enklavu (eng. Secure enclave) ili hardverski podržano skladište ključeva (eng. Hardware-backed Keystore) njegovog uređaja i pristupa mu se putem lokalne biometrijske autentifikacije kad god se ključ koristi za potpisivanje. Ključ ostaje na uređaju i ne postoji način za izvoz privatnog ključa sa uređaja.
- Biblioteke programera (eng. Developer libraries) su način na koji bi programeri aplikacija integrirali podršku za uPort u svoje aplikacije.

Ova tri elementa su “uPort” dio slojevite arhitekture za decentralizirani identitet dat u 7. Osim ova tri elementa, tu su i sloj za aktere/ekstenzije, blockchain sloj i sloj za pohranu datoteka.

F. ShoCard

ShoCard arhitektura je također slojevita. Oni definišu četiri sloja data u 8. Ovi slojevi su [26]:

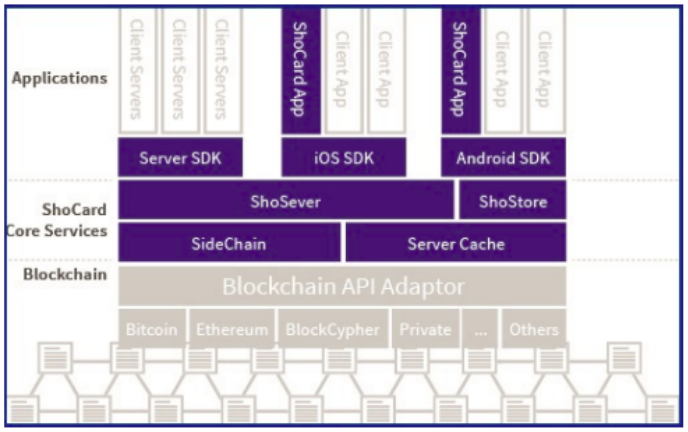
1) ShoCard aplikacije - Sloj ShoCard aplikacija, novčanika, mobilnih aplikacija itd.
2) ShoCard osnovne usluge (eng. ShoCard core services) - Ovaj sloj je odgovoran za upravljanje interfejsom između svih klijentskih SDK-ova (eng. Software Development Kit) i blockchain-a. ShoCard server djeluje



Slika 7. uPort slojevita arhitektura [25]

kao siguran komunikacijski kanal i jednostavno upisuje informacije u blockchain. ShoCard bočni lanci (eng. sidechains) se koriste za povećanje propusnosti. Podaci o certifikaciji pohranjeni su u bočnom lancu, a samo heširani podaci se pohranjuju u javnom blockchainu.

3) Blockchain API adapter - ShoCard Blockchain Adapter apstrahuje sučelje na blockchain-u koje podržava Proof of Work, tako da ShoCard Service sloj može ostati efikasan.
4) Blockchain sloj (Bitcoin, Ethereum, BlockCypher, Private blockchain) – ShoCard koristi nepromjenjivi javni blockchain za provjeru identiteta korisnika, ali ne i za pohranu podataka o korisnicima. Budući da javni blockchain podaci pružaju visok nivo transparentnosti, podaci pohranjeni u blockchainu bi se trebali koristiti samo za provjeru korisničkih certifikata. Blockchain služi kao skladište certifikata.



Slika 8. ShoCard Architecture [27]

V. Diskusija i zaključak

Posmatrajući različite arhitekture SSI-ja primjećuje se da osnovni gradivni blokovi su prisutni u sklopu svih arhitektura i da je blockchain DLT koji se koristi. Međutim, iako su gradivni blokovi tu, rješenja se razlikuju, radi nedostatka standardizacije. Postavlja se pitanje koja arhitektura će biti prihvaćena i kakve će biti aplikacije i rješenja koja će se graditi na ovim osnovnim blokovima. Ovo sa sobom povlači potrebu za istraživanjima koja će se fokusirati na postizanje masovne prihvaćenosti SSI-a, odnosno na poboljšanje upotrebiljivosti i mogućnosti SSI-a, te fokus na korisničke scenarije i iskustvo.

Pored korisničkog iskustva, postavlja se pitanje da li s korisničkog aspekta SSI treba biti mobilna aplikacija. SSI treba biti dostupan i na web preglednicima. U obzir se treba uzeti i nestabilna konekcija na Internet prilikom korištenja SSI.

Predložene arhitekture su najčešće slojevite, pri čemu su u nekim rješenjima određeni slojevi razdvojeni, dok su u drugim povezani. Postojanje i prihvaćenost slojevite arhitekture dozvoljava i poštivanje jednog od osnovnih principa digitalnog identiteta, a to je interoperabilnost. Uvođenjem standardizovanog komunikacijskog sloja sa tačno definisanim ulogama i intefejsima može se postići interoperabilnosti između različitih SSI rješenja.

Postoje alternative za korišteni DLT za implementaciju SSI. One uključuju Hashgraph, Iota Tangle i R3 Corda. I Iota i Hashgraph koriste usmjerene aciklične grafove (DAG) kao alternativnu strukturu podataka za održavanje baze. Svaki od navedenih DLT-ova ima predloženo SSI rješenje [28]–[30]. Detalji o njihovoj arhitekturi su oskudni i zbog toga nisu navedeni u ovom radu. Postavlja se pitanje da li je moguće postići interoperabilnost u slučaju korištenja različitih DLT-ova i naravno da li je zaista blockchain najbolje DLT rješenja za SSI.

Posmatrajući tôk jednog SSI scenarija, možemo uočiti potencijalne probleme koji mogu nastati u manjku standardizacije i definisanih legalnih okvira djelovanja SSI-a. Obzirom da je korisnik taj koji dijeli svoje "verifikovane, digitalno potpisane" podatke, postoje kompanije/vlade koje mogu prikupljati iste informacije i koristiti za vlastite potrebe. Pored toga, sigurnost koja se postiže s enkriptovanim peer-to-peer kanalima otvara prostor kriminalcima da izbjegnu organe vlasti [31].

Kroz scenario i osnovne blokove, možemo vidjeti da je i početna autorizacija korisnika problematična. Pored nje, postoji mogućnost phishing napada prilikom slanja potvrda. Samim tim, radi se na rješenjima koja će kombinirati koncept dokazivanja bez otkrivanja (eng. zero-knowledge proof) i SSI-a. Problemi delegacija, odnosno punomoći je isto tako tekući problem u SSI. Na koji način će neko moći predstavljati drugu osobu koja je onemogućena da sama upravlja svojim digitalnim identitetom, je vodeće pitanje u istraživanjima.

Problem koji se aktivno rješava je i problem revokacije potvrda. Trenutačna rješenja nisu još standardizovana, i njihova skalabilnost je upitna kada se SSI masovno prihvati.

Uvođenje SSI-a da se koristi na državnim nivoima i u sklopu državnih institucija, zahtjeva definisanje odgovarajućih zakona, pravila i normativa za korištenje SSI-a.

U ovom istraživanju date su SSI komponente i različiti pristupi SSI arhitekturi. Budući rad će se fokusirati na definiranju, implementaciji i poboljšanju postojećih SSI rješenja. Jedan od najranijih radova o Self-Sovereign Identity [32] uključuje sljedeći citat: "Na isti način na koji ljudi započinju fizički život posedovanjem izvoda iz matične knjige rođenih, ljudi bi trebali započeti digitalni život sa samoupravljivim identitetom". Pred nama je dug put do stvaranja takvog svijeta, ali razumi-

jevanjem SSI-ja i standardizacijom njegovih komponenti i arhitekture korak smo bliže njegovom postizanju.

LITERATURA

[1] K. C. Toth and A. Anderson-Priddy, "Self-sovereign digital identity: A paradigm shift for identity," *IEEE Security & Privacy*, vol. 17, no. 3, pp. 17–27, 2019.

[2] Čučko and M. Turkanović, "Decentralized and self-sovereign identity: Systematic mapping study," *IEEE Access*, pp. 1–1, 2021.

[3] D. Van Bokkem, R. Hageman, G. Koning, L. Nguyen, and N. Zarin, "Self-sovereign identity solutions: The necessity of blockchain technology," *arXiv preprint arXiv:1904.12816*, 2019.

[4] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, p. 21260, 2008.

[5] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2084–2123, 2016.

[6] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, "A survey on essential components of a self-sovereign identity," *Computer Science Review*, vol. 30, pp. 80–86, 2018.

[7] X. Xu, C. Pautasso, L. Zhu, Q. Lu, and I. Weber, "A pattern collection for blockchain-based applications," in *Proceedings of the 23rd European Conference on Pattern Languages of Programs*, 2018, pp. 1–20.

[8] K. C. Toth and A. Anderson-Priddy, "Architecture for self-sovereign digital identity," in *Proc. 31st Int. Conf. Computer Applications for Industry and Engineering (CAINE)*, 2018.

[9] S. Y. Lim, P. T. Fotsing, A. Almasri, O. Musa, M. L. M. Kiah, T. F. Ang, and R. Ismail, "Blockchain technology the identity management and authentication service disruptor: a survey," *International Journal on Advanced Science, Engineering and Information Technology*, vol. 8, no. 4-2, pp. 1735–1745, 2018.

[10] J. Kaneriya and H. Patel, "A comparative survey on blockchain based self sovereign identity system," in *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)*. IEEE, 2020, pp. 1150–1155.

[11] K. Gilani, E. Bertin, J. Hatin, and N. Crespi, "A survey on blockchain-based identity management and decentralized privacy for personal data," in *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*. IEEE, 2020, pp. 97–101.

[12] O. Dib and K. Toumi, "Decentralized identity systems: architecture, challenges, solutions and future directions," *Annals of Emerging Technologies in Computing (AETiC), Print ISSN*, pp. 2516–0281, 2020.

[13] Y. Liu, Q. Lu, H.-Y. Paik, and X. Xu, "Design patterns for blockchain-based self-sovereign identity," in *Proceedings of the European Conference on Pattern Languages of Programs 2020*, 2020, pp. 1–14.

[14] C. Allen, "The path to self-sovereign identity [www document]," *URL http://www. lifewithalacrity. com/2016/04/the-path-to-self-soverereign-identity. html (accessed 7.4. 20)*, 2016.

[15] "It security and privacy — a framework for identity management — part 1: Terminology and concepts," Standard, May 2019.

[16] [Online]. Available: https://www.w3.org/TR/did-core/

[17] [Online]. Available: https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=379913698

[18] L. Lesavre, P. Varin, P. Mell, M. Davidson, and J. Shook, "A taxonomic approach to understanding emerging blockchain identity management systems," *arXiv preprint arXiv:1908.00929*, 2019.

[19] [Online]. Available: https://www.w3.org/TR/vc-data-model/

[20] M. A. López, "Self-sovereign identity: The future of identity: Self-sovereignity, digital wallets, and blockchain," *Inter-American Development Bank*, vol. 10, p. 0002635, 2020.

[21] "Four architecture pattern candidates for blockchain-based decentralized applications," 4 2019. [Online]. Available: https://www.freecodecamp.org/news/https-medium-com-srinathperera-blockchain-patterns-6cf58fdc2d9b/

[22] "Sovrin glossary v3," 12 2019. [Online]. Available: https://sovrin.org/wp-content/uploads/Sovrin-Glossary-V3.pdf

[23] "In depth introduction to self sovereign identity (ssi)," 6 2020. [Online]. Available: https://labs.hypersign.id/posts/ssi-detail/

[24] "Faqs: Meet the evernym product suite," 2022. [Online]. Available: https://www.evernym.com/blog/faqs-evernym-product-suite/

[25] "All you need to know about uport identity management," 2 2019. [Online]. Available: https://medium.com/@hamzamaslah/all-you-need-to-know-about-uport-identity-management-3fc49db25332

[26] K. Raj, *Foundations of blockchain: the pathway to cryptocurrencies and decentralized blockchain applications*. Packt Publishing Ltd, 2019.

[27] J. Roos, "Identity management on the blockchain," *Network*, vol. 105, 2018.

[28] J. F. Millenaar and M. Yarger, "The case for a unified identity," https://files.iota.org/comms/IOTA_The_Case_for_a_Unified_Identity.pdf.

[29] L. Baird, M. Harmon, and P. Madsen, "Hedera: A public hashgraph network & governing council," *White Paper*, vol. 1, 2019.

[30] "The case for self-sovereign identity," 04 2020. [Online]. Available: https://www.r3.com/blog/the-case-for-self-sovereign-identity/

[31] O. van Deventer and R. Joosten, "Self-sovereign identity - the good, the bad and the ugly; may 2019," https://blockchain.tno.nl/blog/self-sovereign-identity-the-good-the-bad-and-the-ugly/.

[32] H. Farahmand, "Blockchain: Evolving decentralized identity design," *Gartner*, 2017.