

UVOD U BLOKČEJN

Prof. dr Aleksandra Labus

aleksandra.labus@matf.bg.ac.rs

aleksandra.labus@fon.bg.ac.rs

Sadržaj

1. Uvod
2. Arhitektura blokčejna
3. Blokčejn platforme i pametni ugovori
4. Metodologija razvoja blokčejn projekata
5. Razvoj decentralizovanih aplikacija
6. Zaključak

Uvod



Uvod

- Razvojem digitalne ekonomije menjaju se načini savremenog poslovanja i razmene digitalnih informacija.
- U svetu digitalizacije, podaci i informacije se intenzivno razmenjuju i javlja potreba da se osigura prenos transakcija kroz mrežu.
- Blokčejn se zasnivaja na:
 - distribuiranom knjigovodstvu – podaci se čuvaju istovremeno na više računara (čvorova) u mreži, bez centralnog autoriteta.
 - kriptografiji – koristi matematičke algoritme za zaštitu podataka, proveru identiteta i bezbedno izvršavanje transakcija.
 - konsensus protokolima – predstavljaju mehanizme kojima učesnici mreže postižu saglasnost o validnosti transakcija i stanju sistema.
 - pametnim ugovorima – programskim kodovima koji automatski izvršavaju unapred definisana pravila i uslove bez posrednika.

Blokčejn

- Blokčejn tehnologija omogućava beleženje finansijskih transakcija u distribuiranoj bazi podataka.
- Transakcije se:
 - 1.izvršavaju pomoću pametnih ugovora,
 - 2.proveravaju kriptografskim metodama,
 - 3.zapisuju u međusobno povezane blokove podataka.
- Jednom upisani podaci ne mogu se naknadno menjati i dostupni su svim učesnicima u blokčejn mreži.

Blokčejn karakteristike

Decentralizacija

Blokčejn funkcioniše kao distribuirana mreža računara bez centralne institucije koja kontroliše sistem.

Bezbednost i pouzdanost

Kriptografske metode štite podatke i omogućavaju stabilan rad sistema.

Transparentnost

Sve transakcije su zabeležene u zajedničkoj digitalnoj knjizi i dostupne su na uvid učesnicima mreže.

Automatizacija

Pametni ugovori omogućavaju automatsko izvršavanje poslovnih procesa.

Nepromenljivost

Jednom upisani podaci u blokčejn ne mogu se naknadno menjati niti brisati, jer su blokovi međusobno kriptografski povezani u lanac.

Sledljivost

Omogućava praćenje porekla i istorije transakcija ili proizvoda kroz ceo sistem.

Anonimnost

Učesnici mreže se identifikuju pomoću kriptografskih ključeva:

- javnih – služe kao adresa za prijem transakcija,
- privatnih – koriste se za digitalno potpisivanje i autorizaciju transakcija.

Distribuiranost

Podaci i transakcije zaštićeni su kriptografskim metodama i čuvaju se na više računara u mreži.

Blokčejn workflow

1. **Postavljanje zahteva za kupovinu ili prodaju** – Korisnici postavljaju zahteve za kupovinu ili prodaju digitalne imovine na tržištu ili platformi za razmenu.
2. **Usklađivanje ponude i tražnje** – Sistem pronalazi odgovarajuće zahteve i povezuje kupce i prodavce na osnovu cene i uslova trgovanja.
3. **Konverzija fiat valute u kriptovalutu** – Korisnici mogu zameniti tradicionalne valute (npr. EUR, USD) za kriptovalute putem platformi za trgovanje.
4. **Prenos sredstava putem digitalnog novčanika** – Digitalni novčanici omogućavaju čuvanje, slanje i prijem digitalne imovine.
5. **Verifikacija transakcije u blokčejn mreži** – Transakcije proveravaju učesnici mreže primenom konsensus mehanizama.
6. **Dodavanje transakcije u blok i blokčejn** – Potvrđene transakcije zapisuju se u blok i trajno povezuju sa postojećim lancem.
7. **Završetak transakcije** – Transakcija postaje trajno evidentirana i dostupna za proveru.

Blokčejn workflow





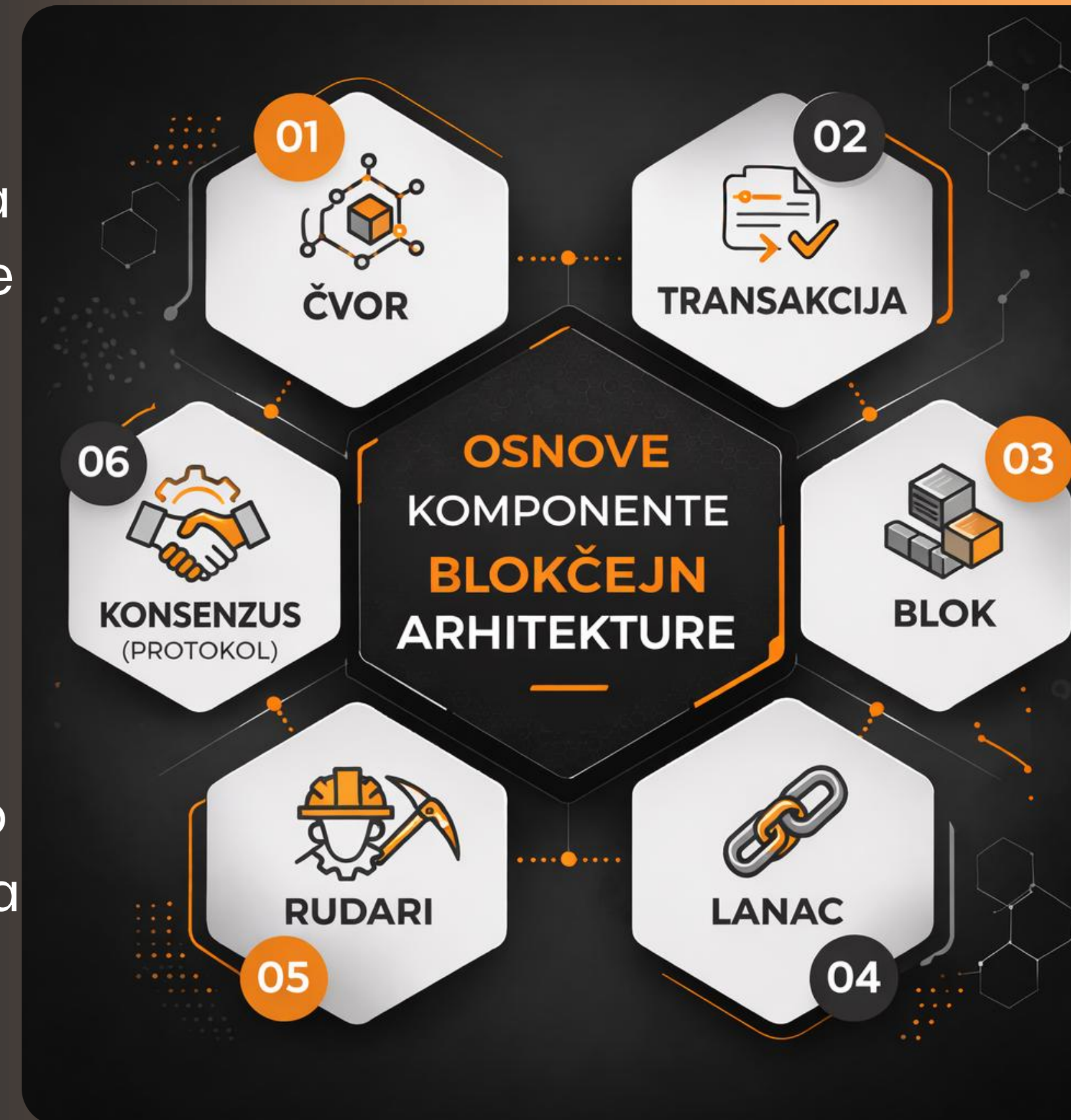
- U upravljanju podacima blokčejn rešava probleme:
 - 1.integriteta,
 - 2.transparentnosti,
 - 3.sledljivosti,
 - 4.poverenja u razmenu i obradu,
 - 5.zaštite od prevara i manipulacija,
 - 6.bezbednosti i privatnosti,
 - 7.interoperabilnosti između različitih sistema.

Arhitektura blokčejna



Arhitektura blokčejna

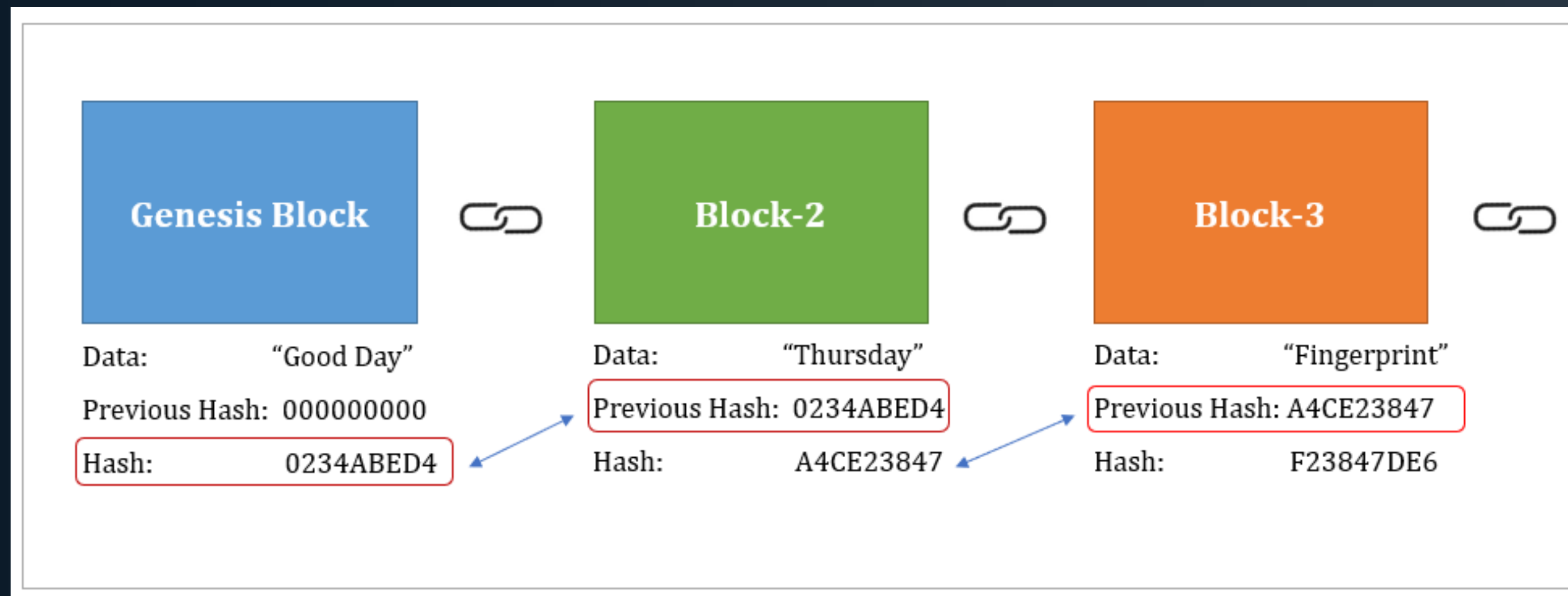
- Nodovi ili čvorovi su pojedinačni računari ili uređaji koji čine blokčejn mrežu.
- Transakcije se razmenjuju između različitih nodova u decentralizovanoj peer-to-peer (P2P) mreži, gde se transakcije validiraju i „ulančavaju“ u blokčejn.
- Svaka transakcija predstavlja jedan blok, pri čemu su blokovi povezani lancem.
- Majneri su zaduženi za validaciju novih transakcija i njihovo skladištenje u globalnoj knjizi.
- Konsenzus algoritam je postupak kroz koji svi članovi blokčejn mreže postižu zajednički dogovor o trenutnom stanju distribuirane knjige. Osigurava da su podaci u blokčejnu tačni i dosledni u svim čvorovima.



Blokov

Blokov sadrže:

- zaglavlje bloka – sadrži metapodatke: broj bloka, heš vrednost prethodnog zaglavlja bloka, vremensku oznaku, nonce vrednost (nasumično generisan broj koji se samo jednom može dodeliti) i veličinu bloka. Heš vrednost zaglavlja prethodnog bloka se čuva u zaglavlju bloka trenutnog bloka (tzv. ulančavanje blokova). Prvi blok nema roditeljski blok i naziva se Genesis Block.
- podaci o bloku – sadrži listu transakcija koje su uključene u blok nakon validacije i autentifikacije.



Blokčejn platforme i pametni ugovori



Blokčejn mreže

- Blokčejn mreže predstavljaju skup međusobno povezanih računara (čvorova) koji zajednički čuvaju, proveravaju i razmenjuju podatke bez centralnog autoriteta.
- Učesnici mreže koriste konsenzus algoritme za potvrdu transakcija i održavanje usaglašenosti podataka u sistemu.
- Svaka mreža koristi različite mehanizme validacije transakcija, nivo transparentnosti i bezbednosne modele.
- Odabir mreže zavisi od potreba korisnika, organizacije i poslovnog scenarija primene.
- Blokčejn mreže mogu biti javne, privatne ili hibridne, u zavisnosti od nivoa pristupa, upravljanja i kontrole učesnika.

Tipovi blokčejn mreža

Javni

- Javni blokčejn je decentralizovana mreža kojoj može pristupiti svako ko ima internet vezu i učestvovati u verifikaciji transakcija i održavanju mreže.
- Glavna prednost je transparentnost jer su svi zapisi o transakcijama javno dostupni.
- Nedostatak je ograničena skalabilnost, jer se brzina obrade transakcija može smanjiti ako se poveća broj korisnika mreže.

Privatni

- Privatni blokčejn je mreža sa ograničenim pristupom koja se koristi unutar kompanija ili organizacija, gde samo ovlašćeni učesnici mogu pristupati i upravljati podacima.
- Prednost je brža obrada transakcija zbog manjeg broja učesnika u mreži.
- Nedostatak je manji nivo decentralizacije i transparentnosti, jer jedna organizacija ili mali broj učesnika kontroliše validaciju podataka.

Hibridni

- Hibridni blokčejn kombinuje karakteristike javnog i privatnog blokčejna.
- Koristi se kada kompanija ili organizacija želi da deo podataka bude javan, a deo dostupan samo određenim učesnicima.

Blokčejn platforme

- Blokčejn platforme predstavljaju tehnološka okruženja zasnovana na blokčejn mrežama koja omogućavaju:
 - ✓ realizaciju transakcija,
 - ✓ razvoj decentralizovanih aplikacija (DApps),
 - ✓ izvršavanje pametnih ugovora i
 - ✓ upravljanje digitalnom imovinom i tokenima.
- Platforme koriste različite konsenzus algoritme, kriptografske metode i mehanizme validacije transakcija radi obezbeđivanja sigurnosti i pouzdanosti sistema.
- Odabir platforme zavisi od poslovnih zahteva, performansi, troškova, brzine obrade i funkcionalnosti koje platforma podržava.

Karakteristike blokčejn platformi

1. **Bezbednost.** Blokčejn platforme koriste kriptografske metode za zaštitu podataka i transakcija. Primeri:

- Hash funkcije (SHA-256) – koriste se u Bitcoin mreži za povezivanje blokova i proveru integriteta podataka.
- Digitalni potpisi (ECDSA, EdDSA) – koriste se za potvrdu identiteta pošiljaoca i autorizaciju transakcija.
- Javni i privatni ključevi – javni ključ predstavlja adresu za prijem sredstava, dok privatni omogućava potpisivanje transakcija.

2. **Transparentnost.** Zavisi od tipa blokčejn mreže:

- Platforme zasnovane na javnim blokčejn mrežama (npr. Bitcoin, Ethereum) omogućavaju visok nivo transparentnosti, jer svi učesnici mogu videti istoriju transakcija.
- Platforme zasnovane na privatnim blokčejn mrežama (npr. Hyperledger Fabric) omogućavaju pristup podacima samo ovlašćenim učesnicima.
- Platforme zasnovane na hibridnim blokčejn mrežama kombinuju javni i privatni pristup, pri čemu su određeni podaci dostupni svim učesnicima, dok su osetljive informacije ograničene.

Karakteristike blokčejn platformi

3. Podrška za pametne ugovore. Ključna karakteristika je autonomnost, jer se ugovori izvršavaju automatski bez posrednika kada su ispunjeni unapred definisani uslovi.

Njihov životni ciklus obuhvata:

- definisanje uslova,
- programiranje,
- implementaciju na blokčejn mrežu i
- automatsko izvršavanje transakcija.

Ethereum najčešće koristi Solidity i Vyper, Solana koristi Rust, dok poslovne platforme poput Hyperledger Fabric često koriste Go, Java i JavaScript.



Karakteristike blokčejn platformi

4. **Skalabilnost.** Predstavlja mogućnost blokčejn platforme da obradi veliki broj transakcija u kratkom vremenskom periodu. Primeri:

- Bitcoin → približno 7 transakcija u sekundi
- Ethereum → približno 15–30 transakcija u sekundi
- Solana → hiljade transakcija u sekundi

5. **Interoperabilnost.** Predstavlja mogućnost komunikacije i razmene podataka između različitih blokčejn platformi, mreža i informacionih sistema:

- API interfejsi omogućavaju povezivanje sa spoljnim sistemima.
- Cross-chain protokoli omogućavaju razmenu podataka između različitih blokčejn mreža i platformi.
- Bridge mehanizmi prenose digitalnu imovinu između blokčejna mreža i platformi.

Primeri:

- Polkadot – povezuje različite blokčejn mreže i platforme.
- Cosmos – omogućava komunikaciju između nezavisnih blokčejn mreža.

Karakteristike blokčejn platformi

6. Konsenzus mehanizmi. Predstavljaju mehanizme koji omogućavaju učesnicima blokčejn mreže da postignu saglasnost o validnosti transakcija i dodavanju novih blokova u sistem.

Koriste se za:

- potvrđivanje validnosti transakcija
- sprečavanje dvostrukog trošenje sredstava
- obezbeđivanje sigurnosti i integriteta mreže
- održavanje usaglašenosti svih čvorova u sistemu

Rešavaju probleme:

- poverenja između učesnika bez centralnog autoriteta
- problem dvostrukog trošenja digitalne imovine
- problem manipulacije podacima i lažnih transakcija
- problem postizanja saglasnosti u distribuiranim sistemima.

Karakteristike blokčejn platformi

6. **Konsenzus mehanizmi.** Predstavljaju mehanizme koji omogućavaju učesnicima blokčejn platformi da postignu saglasnost o validnosti transakcija i dodavanju novih blokova u sistem.

Koriste se za:

- potvrđivanje validnosti transakcija
- sprečavanje dvostrukog trošenje sredstava
- obezbeđivanje sigurnosti i integriteta sistema
- održavanje usaglašenosti svih čvorova u sistemu

Rešavaju probleme:

- poverenja između učesnika bez centralnog autoriteta
- dvostrukog trošenja digitalne imovine
- manipulacije podacima i lažnih transakcija
- postizanja saglasnosti u distribuiranim sistemima.

7. **Troškovi transakcija.** Blokčejn platforme koriste različite modele obračuna naknada za obradu i potvrdu transakcija:

- Bitcoin transaction fee zavisi od opterećenja mreže i prioriteta transakcije.
- Ethereum koristi gas fee koji se plaća u ETH za izvršavanje transakcija i pametnih ugovora.
- Solana – koristi naknade plaćene u SOL tokenima i karakterišu je niski troškovi transakcija.

Tipovi konsenzus algoritama

Zasnovani na rudarenju

- Učesnici mreže koriste računarske resurse za rešavanje kriptografskih zadataka radi potvrde transakcija i dodavanja novih blokova.
- Proof of Work (PoW) – rudari koriste računarske resurse za rešavanje kriptografskih zadataka, potvrdu transakcija i dodavanje novih blokova u lanac.
- Koriste ga Bitcoin, Litecoin, Monero, Dogecoin.

Zasnovani na validatorima

Validatori potvrđuju transakcije na osnovu unapred definisanih pravila, bez potrebe za rudarenjem.

- **Proof of Stake (PoS)** – zaključavaju (staking) deo svojih digitalnih sredstava kao garanciju za učešće u validaciji transakcija, a sistem bira validatore za potvrdu transakcija. Koriste ga:
 - **Ethereum** – validatori koriste uloženi ETH za potvrdu transakcija.
 - **Cardano** – koristi staking za izbor validatora.
 - **Polkadot** – validatori potvrđuju transakcije na osnovu staking mehanizma i izbora validatora.
- **Delegated Proof of Stake (DPoS)** – korisnici glasaju i biraju predstavnike koji u njihovo ime potvrđuju transakcije. Koriste ga:
 - **EOS** – delegati potvrđuju transakcije i održavaju mrežu.
 - **TRON** – koristi izabrane predstavnike za validaciju blokova.
- **Practical Byzantine Fault Tolerance (PBFT)** – PBFT omogućava grupi poznatih učesnika da kroz međusobnu komunikaciju postignu saglasnost o validnosti transakcija. Koristi ga **Hyperledger Fabric**.
- **Proof of History (PoH)** – koristi vremenske oznake za određivanje redosleda događaja i transakcija, dok Solana kombinuje PoH sa PoS mehanizmom za izbor validatora i potvrdu transakcija.

Karakteristike blokčejn platformi

7. Troškovi transakcija. Blokčejn platforme koriste različite modele obračuna naknada za obradu i potvrdu transakcija.

Platforma	Konsenzus	Kriptovaluta / token	Naknada za transakcije	Potrošnja energije	Brzina
Bitcoin	PoW	BTC – plaćanje transakcija i nagrađivanje rudara	Transaction fee (BTC)	Veoma visoka	~7 TPS – Veoma niska
Ethereum	PoS	ETH – plaćanje transakcija, pametni ugovori i staking	Gas fee (ETH)	Niska	~15–30 TPS – Niska
Solana	PoS + PoH	SOL – plaćanje transakcija i staking	Transaction fee (SOL)	Niska	Hiljade TPS – Veoma visoka
Cardano	PoS	ADA – plaćanje transakcija i staking	Transaction fee (ADA)	Niska	~ 250 TPS – Srednja
Polkadot	PoS	DOT – validacija, staking i upravljanje mrežom	Transaction fee (DOT)	Niska	~1000 + TPS – Visoka
Hyperledger Fabric	PBFT	Nema nativnu kriptovalu	Uglavnom nema javnih naknada	Veoma niska	~1000 + TPS – Veoma visoka
VeChain	PoA	VET + VTHO – VET predstavlja vrednost, VTHO izvršavanje transakcija	Transaction fee (VTHO)	Veoma niska	100 + TPS – Srednja

***TPS (Transactions Per Second)** – broj transakcija koje mreža može obraditi u jednoj sekundi.

Metodologija razvoja blokčejn projekata

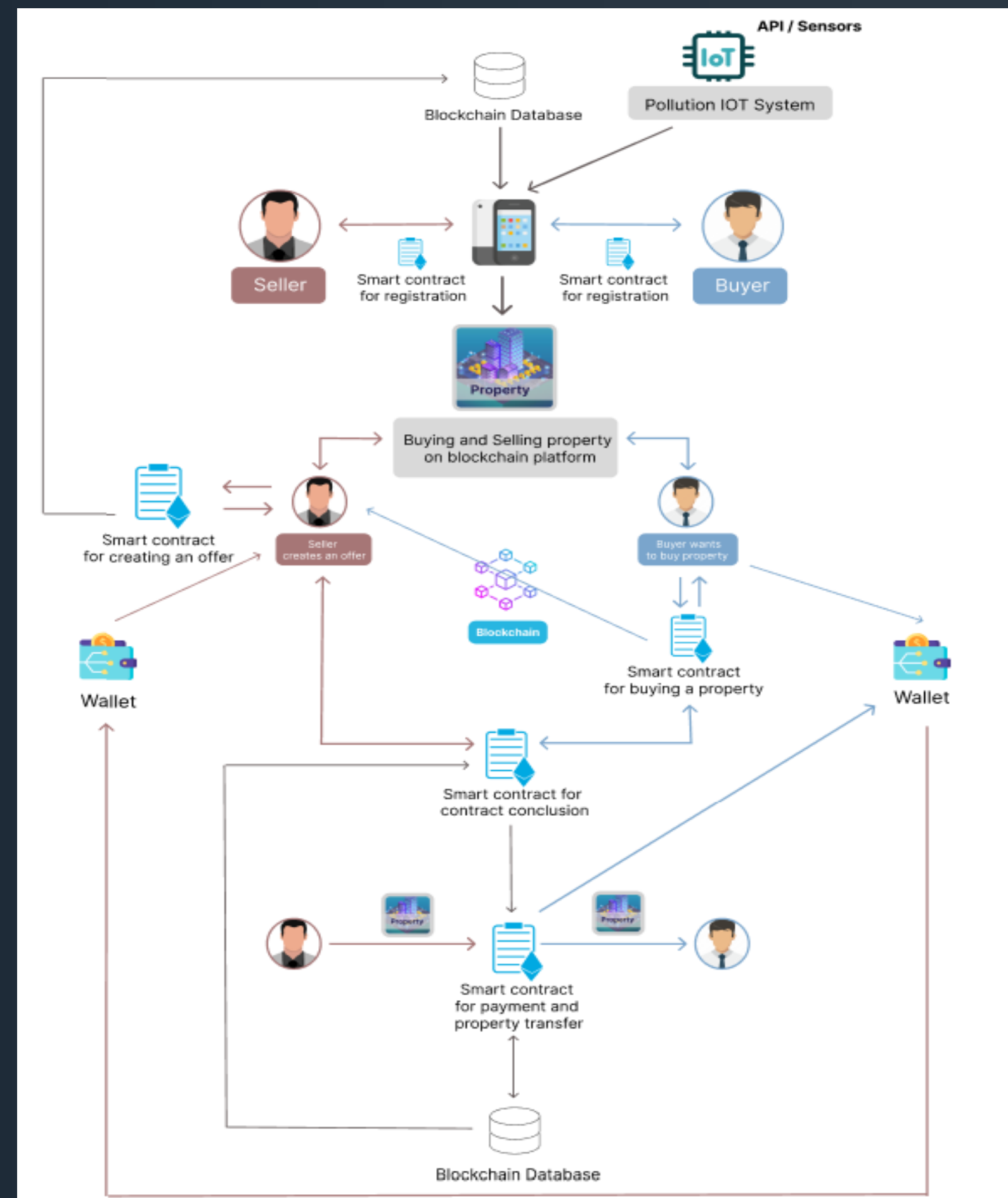


Matodologija razvoja blokčejn projekata



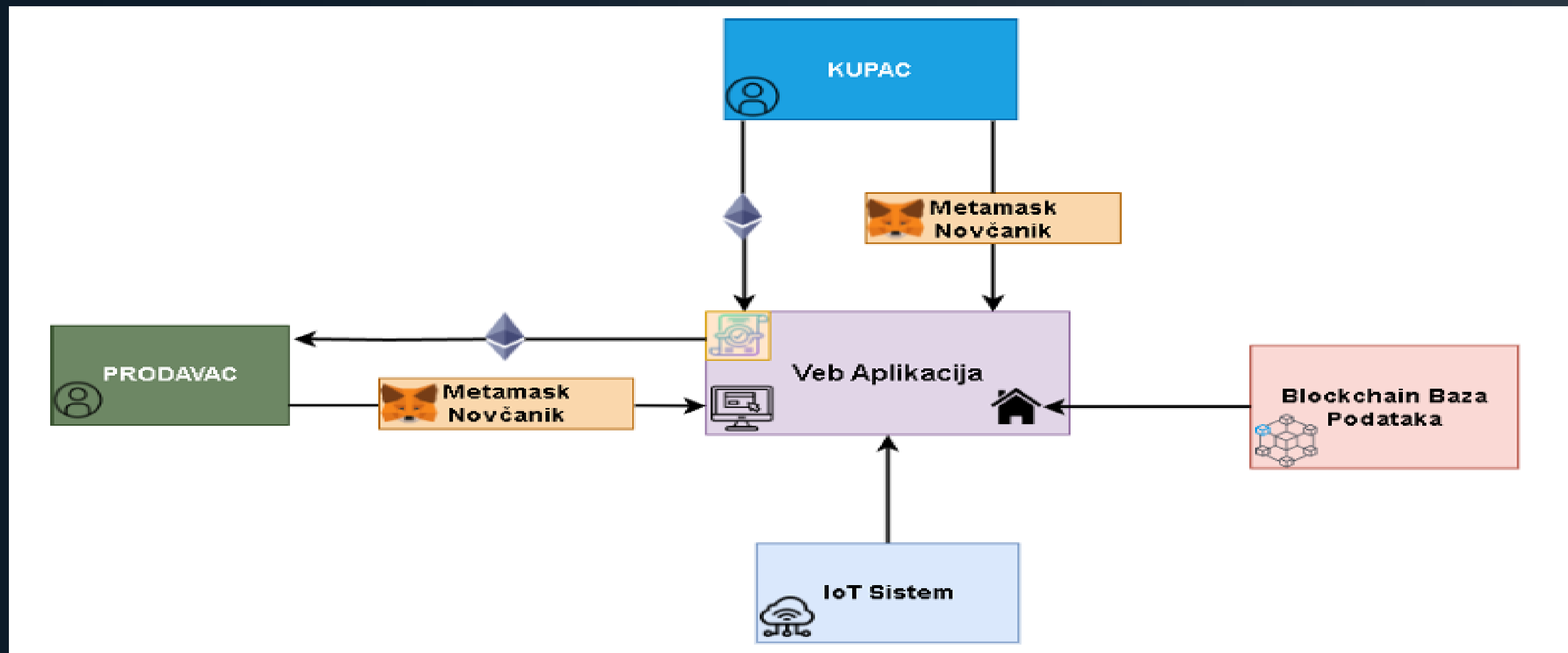
Definisanje ekosistema zasnovanog na blokčejnu

- Definisanje ekosistema zasnovanog na blokčejnu obuhvata:
 1. Identifikaciju svih učesnika ekosistema
 2. Analizu poslovnih procesa između učesnika
 3. Definisanje uloge blokčejn tehnologije u realizaciji poslovnih transakcija
 4. Prikaz složenih transakcija koje se realizuju između različitih učesnika primenom pametnih ugovora.



Definisanje arhitekture sistema zasnovanog na blokčejnu

- Arhitektura sistema zasnovanog na blokčejnu je konceptualni model koji definiše strukturu, interakciju učesnika i način funkcionisanja sistema.

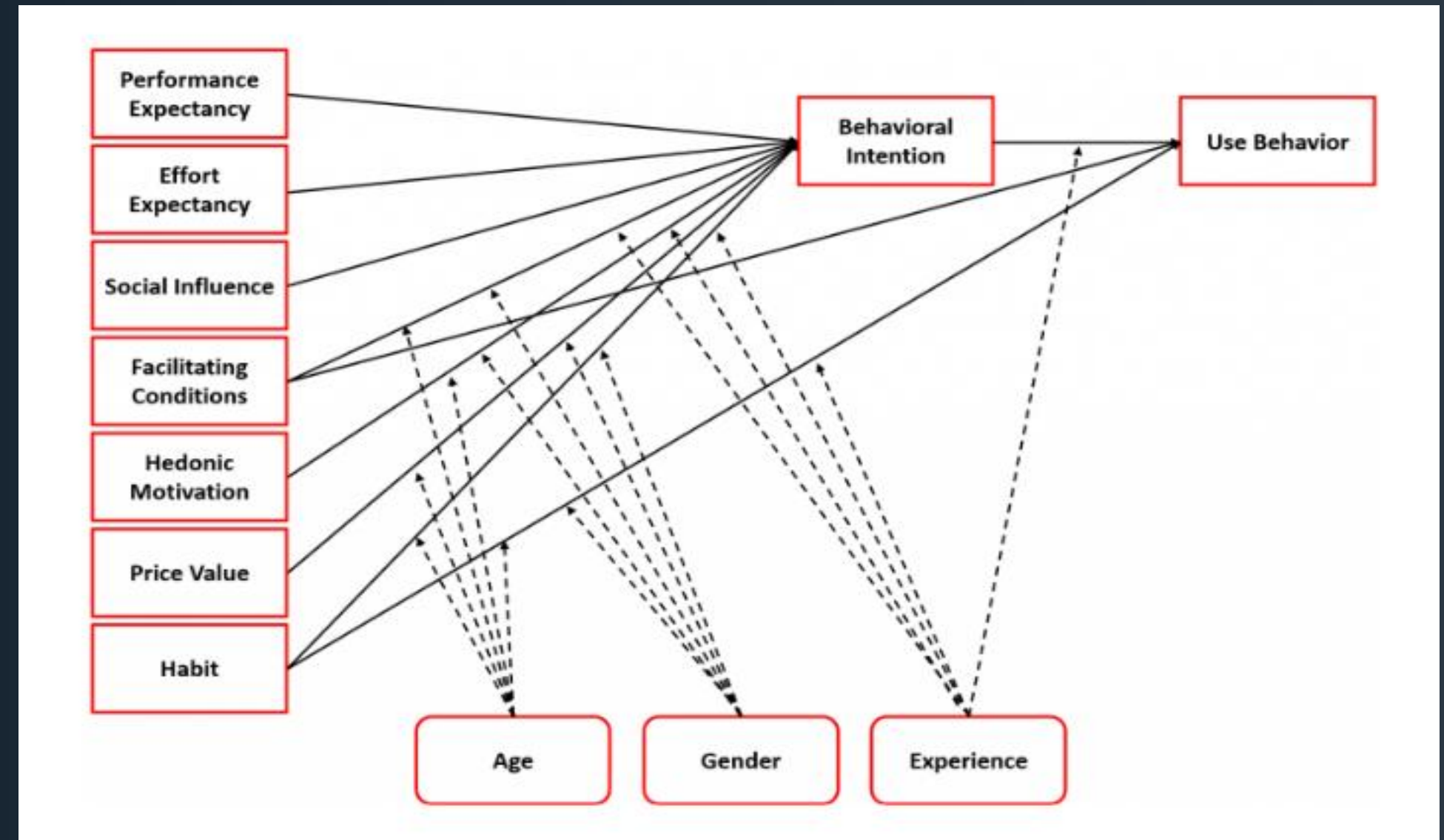


Ispitivanje spremnosti uvođenja blokčejn tehnologije

- Za ispitivanje spremnosti uvođenja nove tehnologije kao što je blokčejn mogu se koristiti sledeće metode:
 1. TAM (Technology Acceptance Model) – model koji je fokusiran na osnovne komponente korisnosti i lakoće.
 2. UTAT(2) (Unified Theory of Acceptance and Use of Technology) – model koji uključuje ispitivanje faktora kao što su performanse očekivanja, napor očekivanja, društveni uticaj, i olakšavajući uslovi.
 3. VAM (Value-based Adoption Model) – model koji se fokusira na percepciju korisničke vrednosti tehnologije kroz komponente kao što su percipirana korist i percipirani trošak.
 4. ORIC (Organizational Readiness for Implementing Change) – metode koje se fokusiraju na organizacione kapacitete.

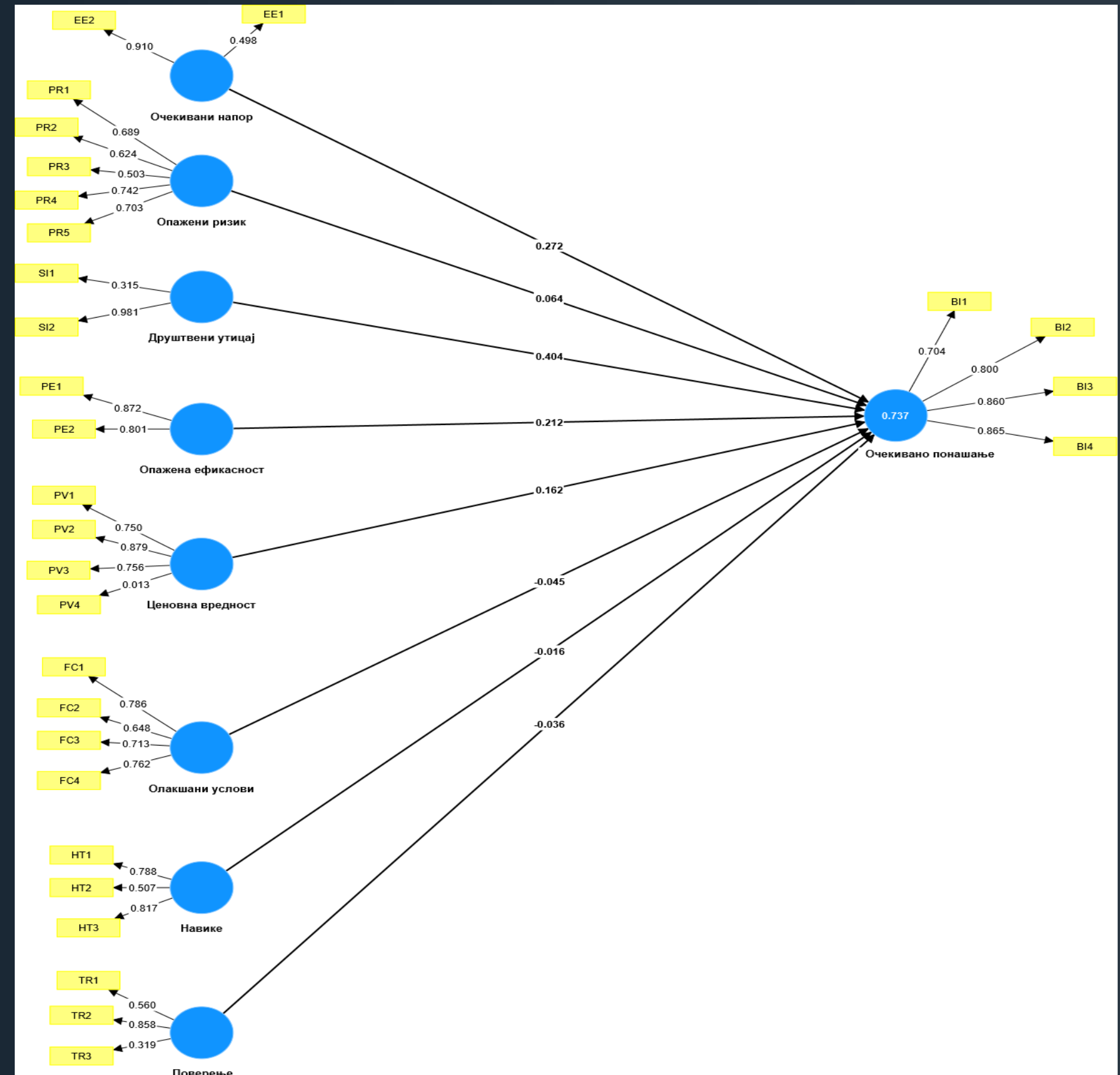
Ispitivanje spremnosti uvođenja blokčejn tehnologije: UTAUT2

- UTAUT2 model se može koristiti za ispitivanje uticaja sledećih varijabli na očekivano ponašanje:
 1. očekivane performanse,
 2. očekivani napor,
 3. društveni uticaj,
 4. olakšavajući uslovi,
 5. hedonistička motivacija,
 6. cenovna vrednost,
 7. navike.



Ispitivanje spremnosti uvođenja blokčejn tehnologije: UTAUT2

- Za analizu podataka obično se koristi SmartPLS softverski alat.
- Pomoću SmartPLS-a se ispituju veze između korišćenih varijabli i očekivanog ponašanja.
- Možemo utvrditi koje su hipoteze više ili manje statistički značajne za primenu blokčejn tehnologije u određenoj oblasti.
- Nakon primene određenih algoritama utvrđuje se da li je postavljeni model dobar i koliko dobro nezavisne varijable objašnjavaju promene u zavisnoj varijabli.



Prikaz modela unutar smartPLS softverskog alata

Definisanje poslovnog modela zasnovanog na blokčeju

- Poslovni model (Business Model Canvas) obezbeđuje osnovu za donošenje strateških odluka, identifikaciju tržišnih segmenata i upravljanje odnosima sa korisnicima.
- Kroz osnovne segmenate poslovnog modela važno je istaknuti kako blokčejn tehnologija unapređuje sigurnost, transparentnost, efikasnost i poverenje.

Кључни партнери	Кључне Активности	Предлог вредности	Однос са корисницима	Сегмент тржишта
- Постојеће агенције за продају и куповину некретнина - Организације које поседују податке о загађењу - Произвођачи сензора - Провјидери који одржавају сервере и хостинг	- Развој IoT система - Развој децентрализоване апликације за паметне градове - Развој фронт енд-а апликације у React.js оквиру - Развој паметних уговора у Solidity програмском језику - Одржавање IoT система и сензора	- Могућност куповине и продаје некретнина путем блокчејн технологије - Увид у ниво загађења унутар паметног града на различитим микролокацијама - Безбедност и транспарентност приликом куповине, коришћењем паметних уговора - Обезбеђено власништво над некретнином	- Обука корисника за коришћење паметних новчаника и web 3.0 - Респонзиван однос са корисницима у континуалну подршку и сервис повратних информација	- Власници некретнина који имају намеру да продају некретнину - Купци који су заинтересовани за живот у паметном граду - Агенције за продају некретнина које траже апликацију која омогућава транспарентну и сигурну куповину уз акценат на екологију и паметан начин живота
Кључне Вредности - Тим програмера који раде на сталном унапређењу фронт и бек енд-а апликације - Инфраструктура система интерната интелигентни уређаја - Подаци који се односе на загађење и на некретнине доступне за куповину - Сервер за хостинг		Канали комуникације - Канали социјалних медија - Партнества са другим агенцијама за продају и куповину некретнина		
Структура трошкова - Трошкови од изнајмљивања сервера и одржавања истих - Трошкови одржавања IoT инфраструктуре - Трошкови маркетинга и промоције апликације - Трошкови обуке запослених програмера, као и плате, за одржавање целокупног система			Структура Прихода - Накнада од агенција које користе овај систем за продају некретнина - Приходи од реклама присутних унутар веб апликације - Провизија од трансакција и куповина остварених коришћењем апликације	

Upravljanje blokčejn projektima

- Metodologija koja je najprikladnija za blokčejn projekte kombinuje tradicionalne principe upravljanja projektima sa specijalizovanim praksama prilagođenim sigurnim i decentralizovanim sistemima.
- Ključni koraci u upravljanju i implementaciji blokčejn projekata su:
 1. Pokretanje projekta i planiranje
 2. Dizajn i razvoj
 3. Lansiranje projekta
 4. Marketing i angažovanje zajednice
 5. Praćenje i evaluacija
 6. Kontinuirano unapređenje i inovacije

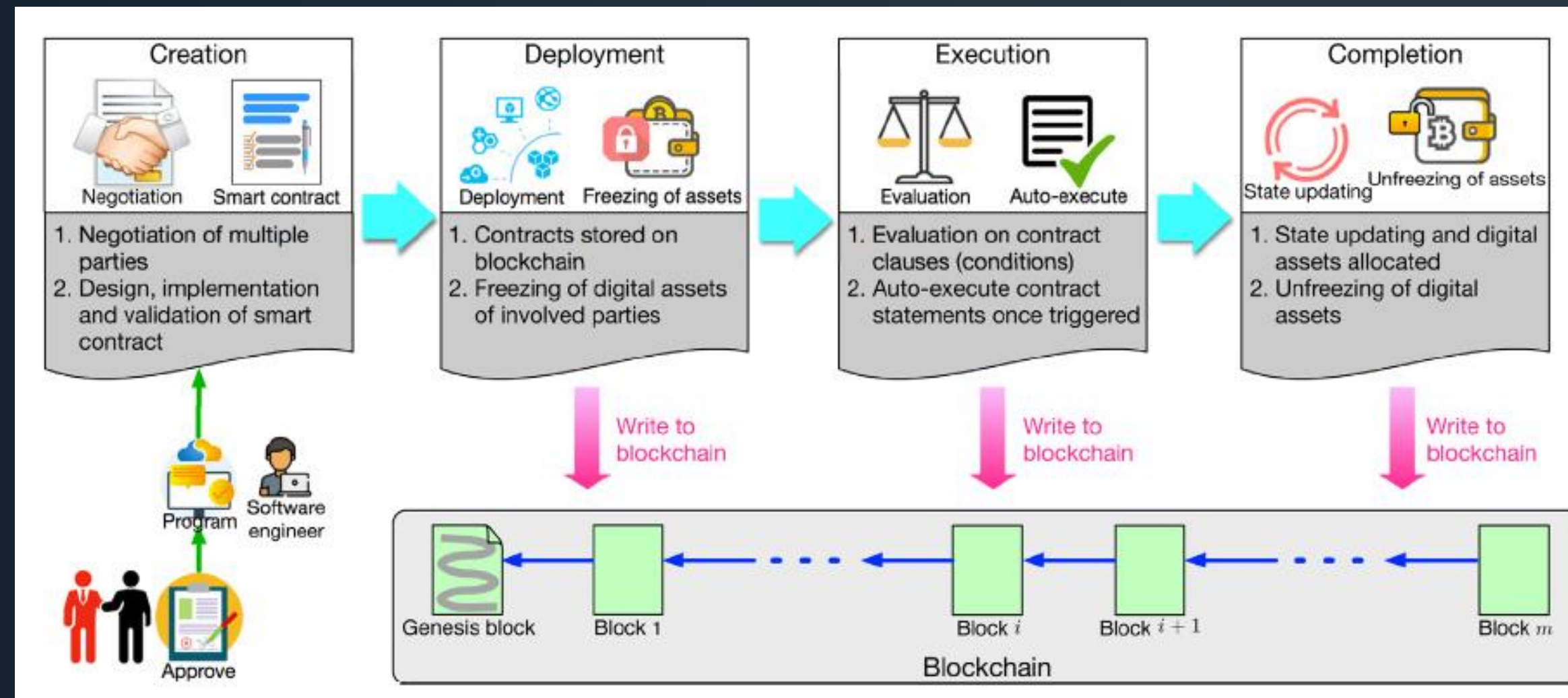
DevOps pristup za upravljanje blokčejn projektima

- DevOps predstavlja kompleksnu metodologiju, skup praksi i alata koji integrišu razvoj softvera (Development) i IT operacije (Operations) sa ciljem automatizacije softverskog procesa, ubrzavanje ciklusa isporuke softvera i poboljšavanje kvaliteta aplikacija.
- Primena DevOps-a u različitim fazama životnog razvoja aplikacije:
 1. Planiranje: Definisanje zahteva aplikacije kroz backlog i praćenje bagova
 2. Razvoj i testiranje: Pisanje, testiranje i verzionisanje koda
 3. Isporuka: Kontinuirana isporuka testiranog koda na produkciju
 4. Održavanje/Podrška: Nadgledanje i podrška aplikacije nakon isporuke



Odabir blokčejn platforme i razvoj pametnih ugovora

- Blokčejn platforme mogu imati dve namene:
 1. Rudarenje kriptovaluta
 2. Realizacija poslovnih transakcija
- Životni ciklus pametnog ugovora sastoji se od:
 - Razvoja pametnog ugovora
 - Primene pametnog ugovora u okviru blokčejn platforme
 - Izvršenja pametnog ugovora
 - Završetka transakcije

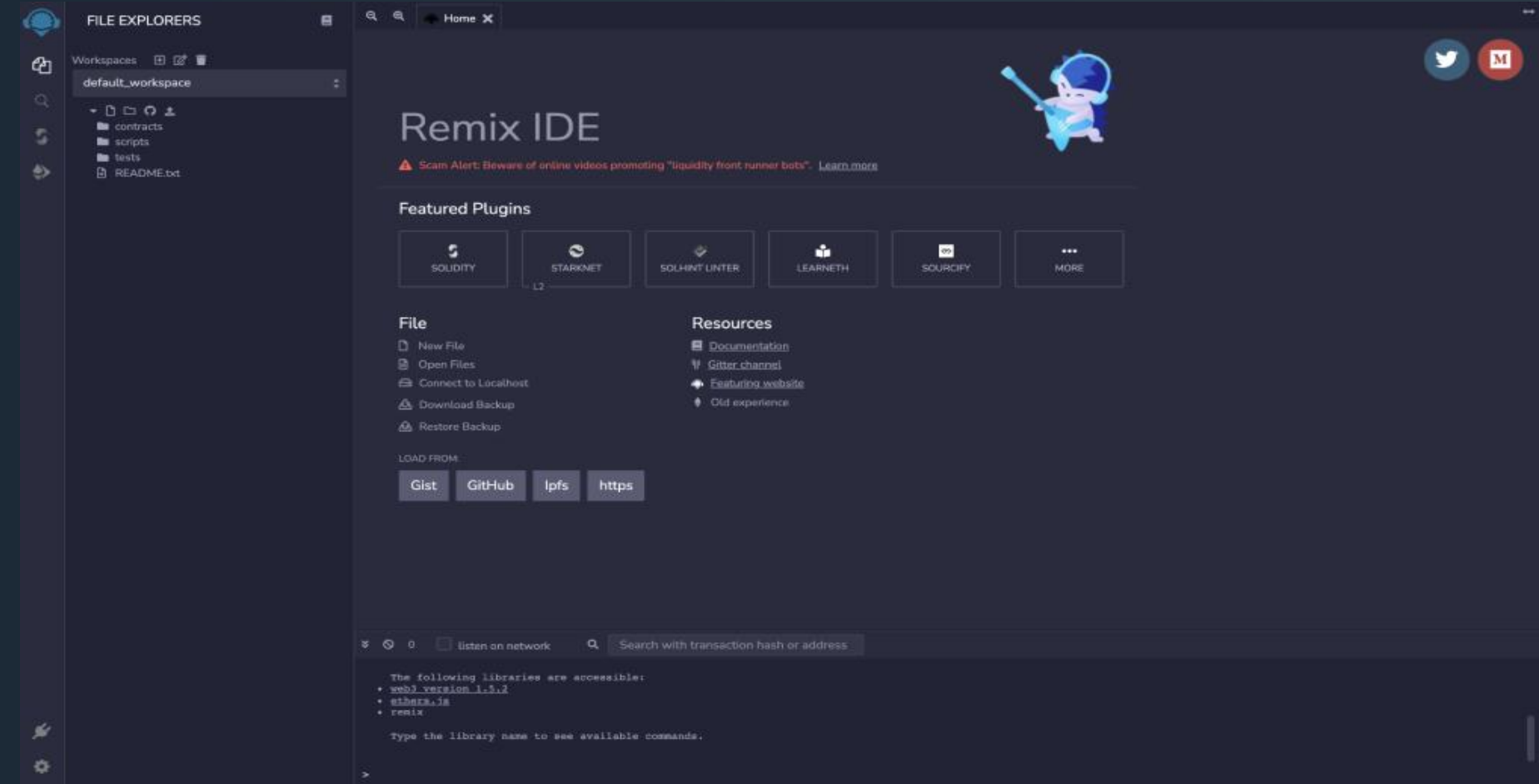


Razvoj pametnih ugovora

1. Definisanje ciljeva i funkcionalnosti koje pametni ugovor treba da obezbedi.
2. Odabir blokčejn platforme koja podržava korišćenje pametnih ugovora.
3. Pisanje koda pametnog ugovora korišćenjem odgovarajućeg programskog jezika.
4. Razvoj i testiranje koda u Remix IDE-u.
5. Postavljanje pametnog ugovora na testnet mrežu kako bi se simuliralo njegovo ponašanje pre implementacije.
6. Nakon uspešnog testiranja, pametni ugovor se postavlja na mainnet kako bi bio dostupan za korišćenje.

Razvoj pametnih ugovora

- **Solidity** je objektno-orijentisani jezik posebno razvijen za pisanje pametnih ugovora na Ethereum blokčejn platformi.
- Razvijen za kreiranje funkcionalnih ugovora koji mogu upravljati vlasništvom, transakcijama i interakcijama između ugovora.
- Solidity se koristi za pisanje verifikovanog koda koji je efikasan u pogledu troškova izvršavanja i transakcija, koristeći funkcije kao što su nasleđivanje, biblioteke i složene korisnički definisane tipove podataka.
- **Remix IDE** je skup alata za razvoj, primenu, otklanjanje grešaka i testiranje pametnih ugovora kompatibilnih za Ethereum.
- Pored toga što omogućava pisanje i testiranje koda pametnih ugovora, Remix takođe pruža pristup alatima za statičku analizu koda, što pomaže u identifikaciji potencijalnih problema pre postavljanja na blokčejn.



Razvoj pametnih ugovora

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract RealEstate {
    address payable private beneficiary;
    uint256 private price;
    int256 private lat;
    int256 private lon;
    string private locationName;
    bool private registered;
    bool private mortgageFree;
    uint256 private sqft;
    string private floor;
    string private heatingType;
    uint256 private numberOfRooms;

    mapping(address => uint) pendingReturns;

    event RealEstateBought(address indexed buyer, uint256 price);
```

Ugovor RealEstate.sol sa atributima

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

import "../RealEstate.sol";

contract RealEstateFactory {
    RealEstate[] public realEstates;

    function createRealEstate(address payable _beneficiary, uint256 _price, int256 _lat, int256 _lon,
        string memory _locationName, bool _registered, bool _mortgageFree, uint256 _sqft, string memory _floor,
        string memory _heatingType, uint256 _numberOfRooms) public {

        RealEstate newRealEstate = new RealEstate(_beneficiary, _price, _lat, _lon, _locationName,
            _registered, _mortgageFree, _sqft, _floor, _heatingType, _numberOfRooms);
        realEstates.push(newRealEstate);
    }

    function getAllRealEstates() public view returns (RealEstate[] memory) {
        return realEstates;
    }
}
```

Ugovor RealEstateFactory.sol sa funkcijama

```
function buyRealEstate() external payable {
    require(!registered, "Property is already registered");
    require(msg.value >= price, "Insufficient funds");

    beneficiary = payable(msg.sender);
    registered = true;

    if (msg.value > price) {
        pendingReturns[msg.sender] += msg.value - price;
    }

    emit RealEstateBought(msg.sender, price);
}
```

Funkcija buyRealEstate za kupovinu nekretnine

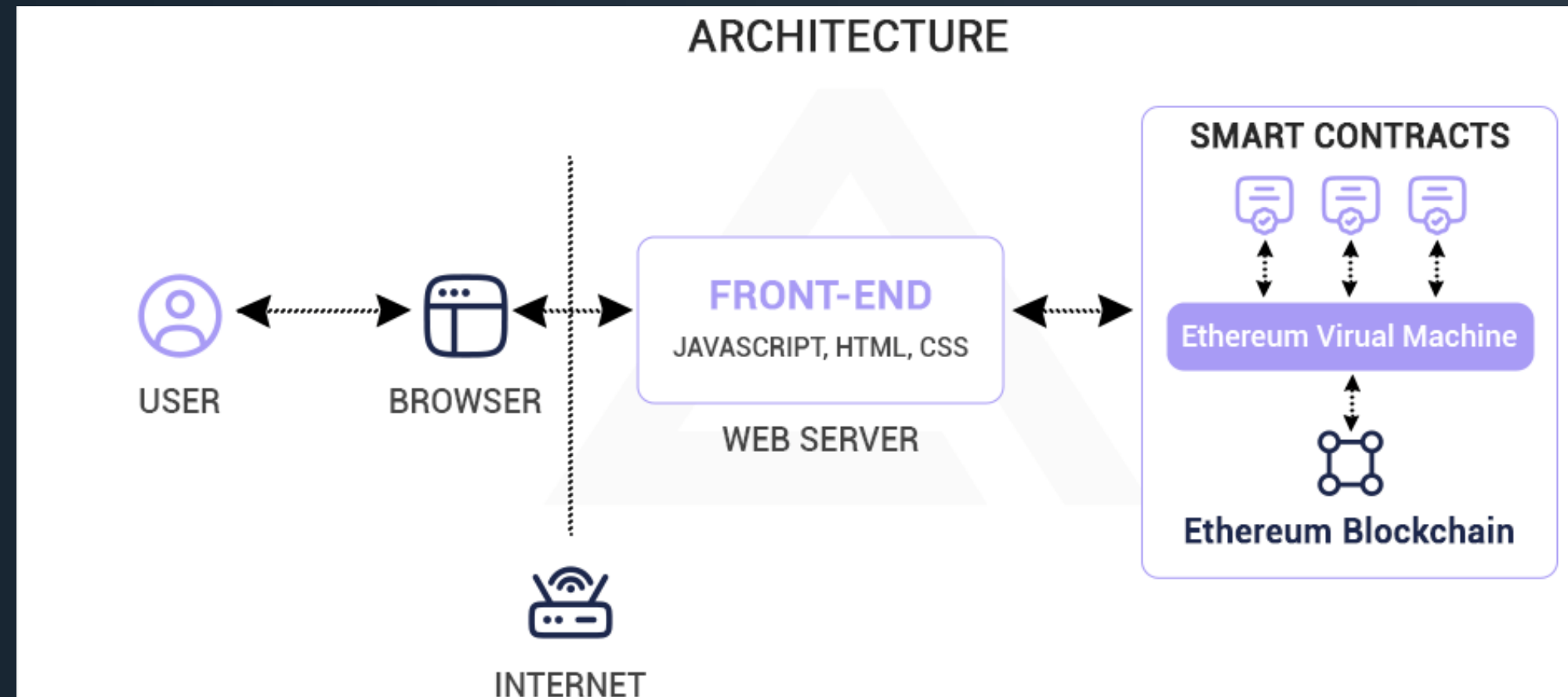
Razvoj decentralizovanih aplikacija - DApps

Decentralizovane aplikacije (DApps) su softverske aplikacije koje funkcionišu na blokčejn platformama i koriste decentralizovanu infrastrukturu, pri čemu se podaci, logika aplikacije i transakcije distribuirano čuvaju i izvršavaju kroz mrežu čvorova, bez centralnog autoriteta.

Ove aplikacije često koriste kriptovalute ili tokene za realizaciju transakcija, izvršavanje pametnih ugovora i pristup određenim funkcionalnostima sistema.

Arhitektura DApps-a obuhvata tri glavna sloja:

1. **Front-end**: korisnički interfejs koji je vrlo sličan tradicionalnim veb aplikacijama.
2. **Pametni ugovori**: predstavljaju back-end logiku aplikacije koja se izvršava na blokčejn platformi i automatski sprovodi unapred definisana pravila i procese.
3. **Blokčejn platforma**: sloj na kome se čuvaju podaci i transakcije, obezbeđujući transparentnost, nepromenljivost i decentralizaciju.



Razvoj decentralizovanih aplikacija



Postupak razvoja decentralizovanih aplikacija

Postupak razvoja DApps-a:

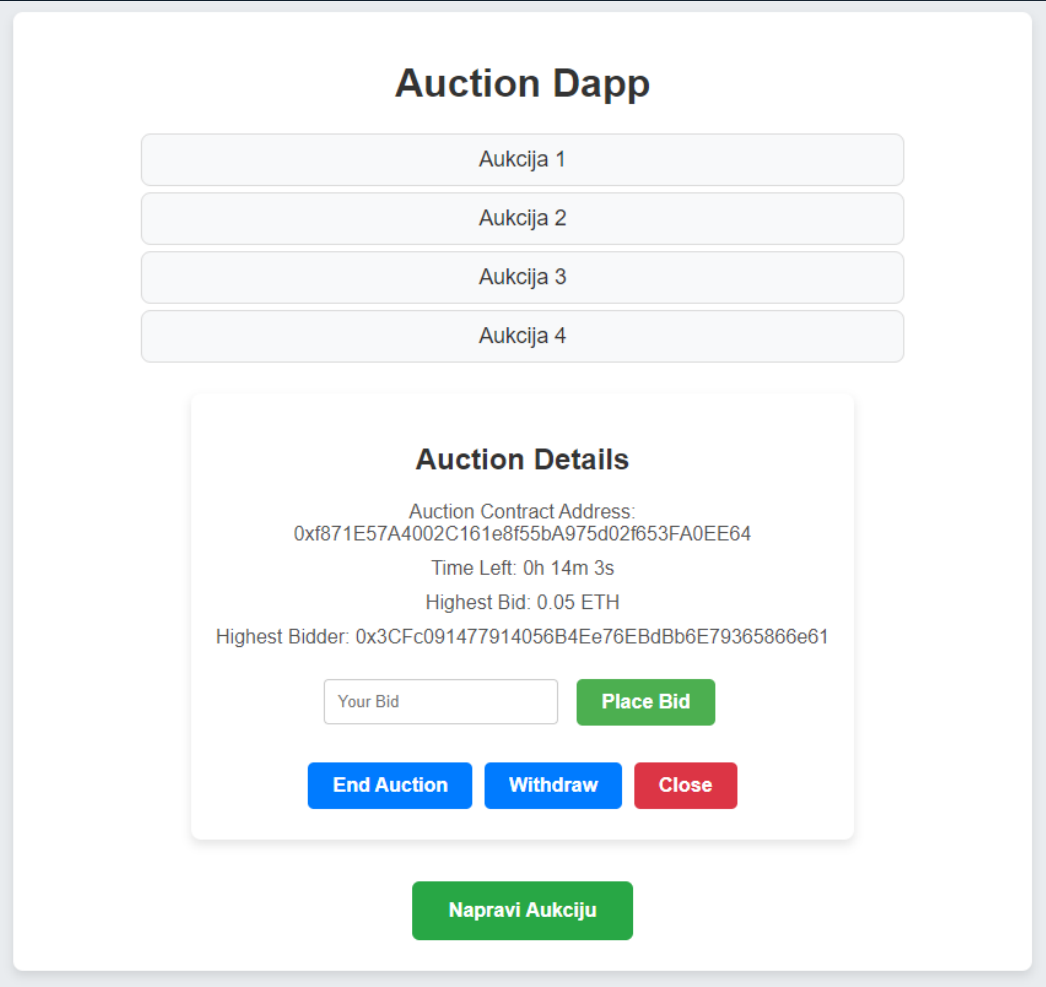
1. Definisanje ciljeva i funkcionalnosti DApp-a
2. Odabir blokčejn platforme
3. Razvoj pametnih ugovora radi automatizacije poslovne logike decentralizovane aplikacije
4. Razvoj korisničkog interfejsa i povezivanje sa pametnim ugovorima
5. Integracija sa digitalnim novčanicima poput MetaMask-a u cilju omogućavanja korisnicima da komuniciraju sa blokčejn platformom i mrežom.
6. Testiranje funkcionalnosti aplikacije i postavljanje na glavnu mrežu (mainnet).

Razvoj front-end dela

- Tehnologije: Za razvoj front-end dela mogu se koristiti JavaScript okviri poput React-a ili Vue.js-a.
- Povezivanje sa blokčejnom: Koriste se biblioteke kao što su Web3.js ili Ethers.js za komunikaciju između korisničkog interfejsa i pametnih ugovora.



```
import Web3 from 'web3';
import './Main.css';
const auctionFactoryAddress = "0x4E171D904a950627014090...";
const sepoliaRPCUrl = 'https://sepolia.infura.io/v3/cde52bf4....';
```



Auction Dapp

Aukcija 1
Aukcija 2
Aukcija 3
Aukcija 4

Auction Details

Auction Contract Address:
0xf871E57A4002C161e8f55bA975d02f653FA0EE64

Time Left: 0h 14m 3s

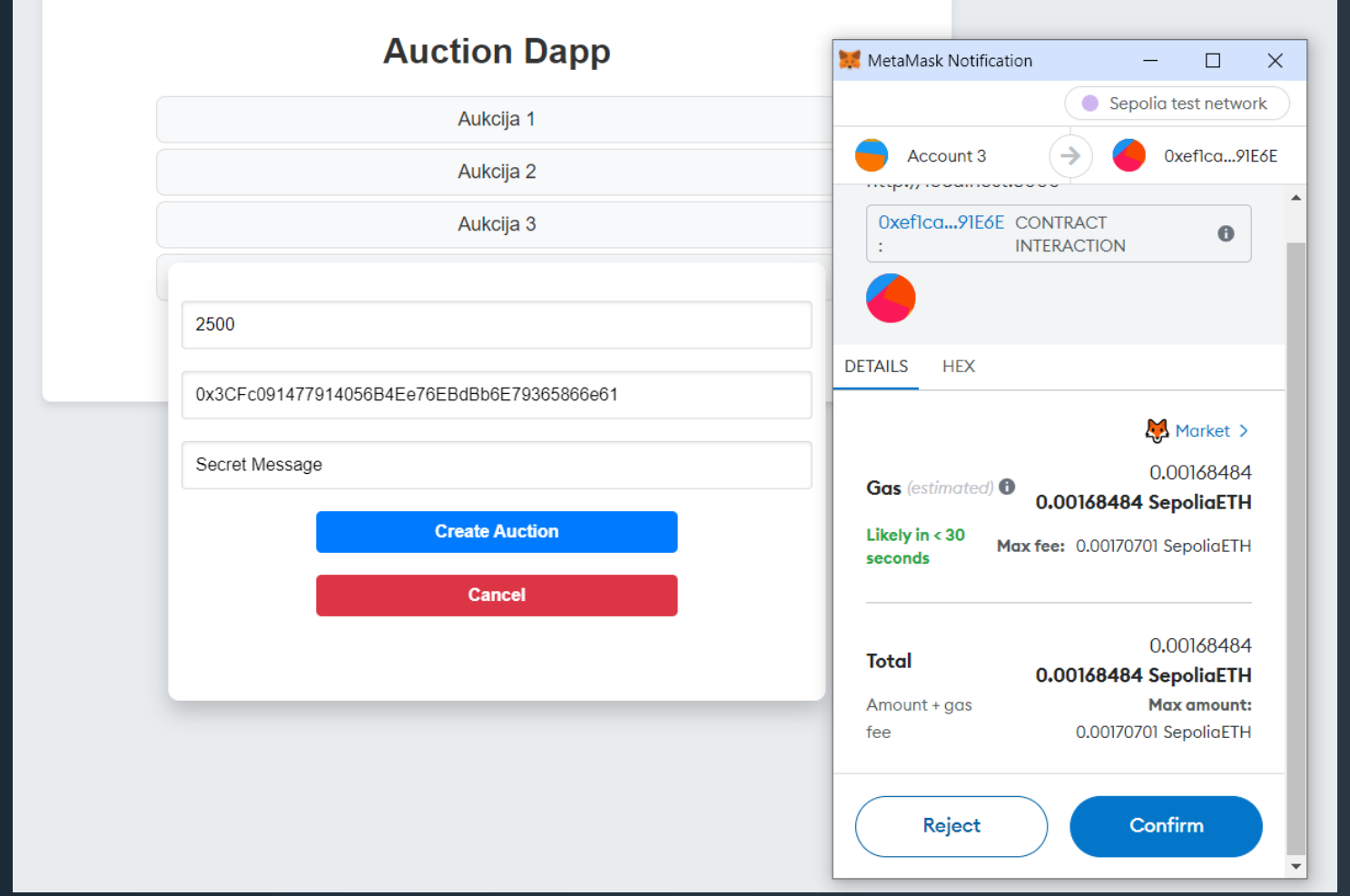
Highest Bid: 0.05 ETH

Highest Bidder: 0x3CFc091477914056B4Ee76EBdBb6E79365866e61

Your Bid **Place Bid**

End Auction **Withdraw** **Close**

Napravi Aukciju



Auction Dapp

Aukcija 1
Aukcija 2
Aukcija 3

2500

0x3CFc091477914056B4Ee76EBdBb6E79365866e61

Secret Message

Create Auction

Cancel

MetaMask Notification

Sepolia test network

Account 3 → 0xeflca...91E6E

0xeflca...91E6E CONTRACT INTERACTION

DETAILS HEX

Market >

Gas (estimated) 0.00168484
0.00168484 SepoliaETH

Likely in < 30 seconds Max fee: 0.00170701 SepoliaETH

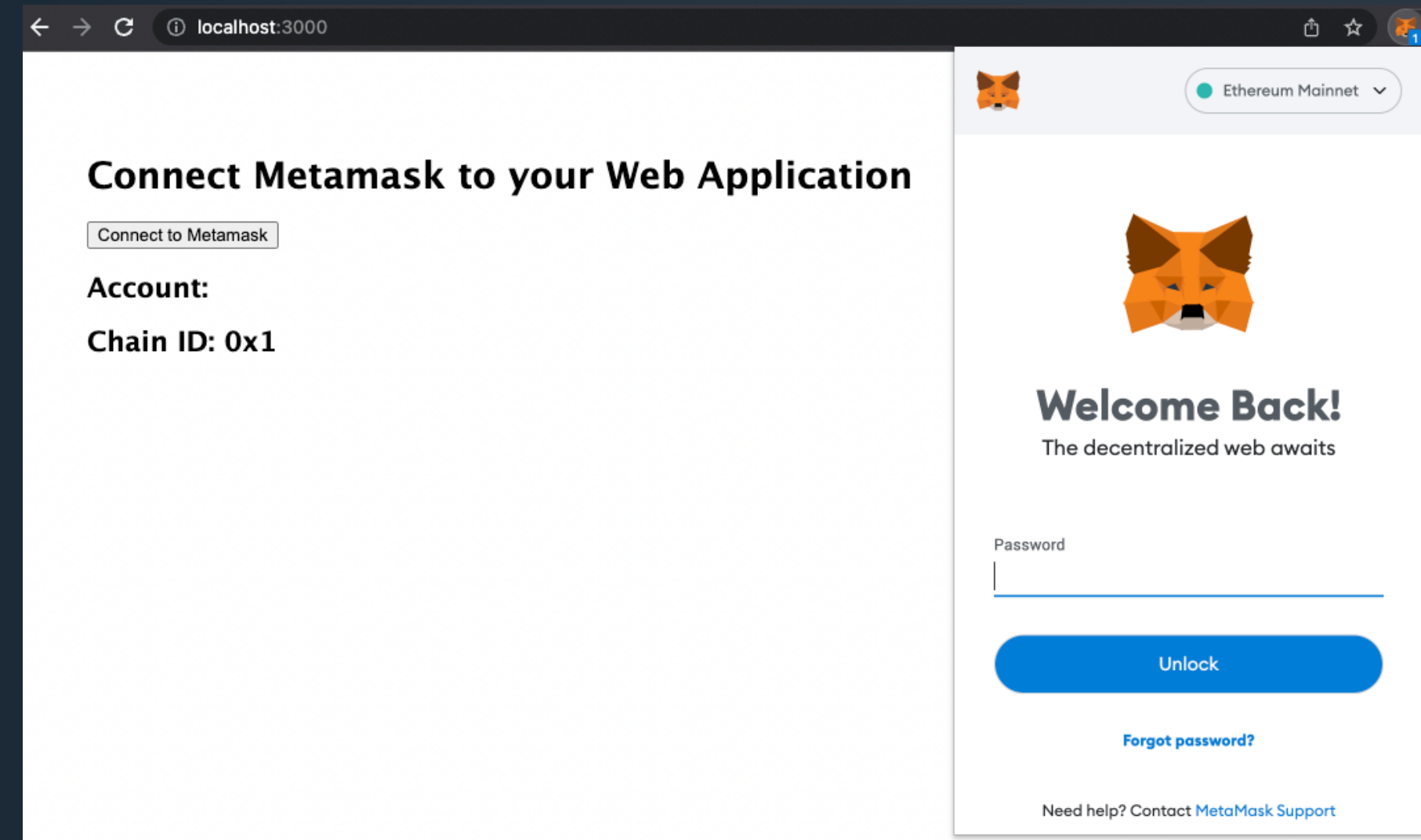
Total 0.00168484
0.00168484 SepoliaETH

Amount + gas fee Max amount:
0.00170701 SepoliaETH

Reject **Confirm**

Integracija sa platnim sistemima

- Plaćanja u okviru decentralizovanih aplikacija su moguća korišćenjem digitalnih novčanika.
- Digitalni novčanici omogućavaju korisnicima da sigurno čuvaju svoje kriptovalute i komuniciraju sa DApp-om.
- Koriste se za prijavljivanje korisnika, potvrđivanje transakcija i upravljanje tokenima.
- Primeri: MetaMask, Trust Wallet, Coinbase Wallet, Ledger
- MetaMask omogućava korisnicima da se povežu sa Ethereum blokčejnom direktno iz njihovog pretraživača.



Konverzija u Ethereum (ETH)

- **Kupovina i konverzija:** Korisnici mogu konvertovati fiat valutu (npr. dolar) u ETH putem **kripto berzi** poput **Binance-a** ili **Coinbase-a**.
- **Upotreba ETH-a:** ETH se koristi za plaćanje transakcija na Ethereum mreži i za interakciju sa pametnim ugovorima.

The screenshot shows the 'Convert & OTC Portal' on the Binance website. It features a 'Market' tab selected, with 'Limit' and 'Orders' options. The 'From' section shows 'Spot wallet available' with a balance of '0.05312269 USDT'. The 'To' section shows a dropdown for 'BTC'. A note at the bottom states: 'the conversion will proceed immediately based on the current market price'.

The 'Confirm' modal displays the conversion details for converting 10 USDT to BNB. It shows the resulting amount of 0.03202642 BNB, the rate (1 USDT = 0.00320264 BNB), the inverse rate (1 BNB = 312.242 USDT), the payment method (Spot wallet), and transaction fees (No Fees). A large yellow button labeled 'Convert(3s)' is at the bottom.

From	To
10 USDT	0.03202642 BNB

Rate ⓘ 1 USDT = 0.00320264 BNB
Inverse Rate 1 BNB = 312.242 USDT
Payment Method Spot wallet
Transaction Fees ⓘ No Fees
You will receive 0.03202642 BNB

Convert(3s)

Preview Conversion

Testiranje DApp-a

Neki od ključnih elemenata za testiranje decentralizovanih aplikacija zasnovanih na blokčejnu obuhvataju:

- Testiranje funkcionalnosti pametnih ugovora: Proveriti pravilno izvršavanje ugovora simulirajući različite scenarije obuhvaćene ugovorom.
- Testiranje na test mrežama: Koristiti testnet mreže (kao što je TESTNET Sepolia za Ethereum) kako bi se simuliralo stvarno okruženje.
- Bezbednosno testiranje: Proveriti aplikaciju za sigurnosne ranjivosti.
- Testiranje korisničkog interfejsa (UI): Osigurati da je korisnički interfejs intuitivan i funkcionalan na različitim uređajima i platformama.
- Opterećenje i skalabilnost: Testirati kako DApp reaguje na veliki broj korisnika i transakcija.

Promocija putem digitalnog marketinga

Neki od ključenih koraka promocije decentralizovane aplikacije jesu:

- Kreiranje sadržaja: Objavljivanje edukativnih i informativnih sadržaja koji objašnjavaju prednosti DApp-a i način njegove upotrebe, čime se povećava svest i razumevanje među korisnicima.
- Angažovanje zajednice na društvenim mrežama: Aktivno prisustvo na platformama omogućava dvosmernu komunikaciju s korisnicima, prikupljanje povratnih informacija i izgradnju poverenja u zajednici.
- Korišćenje kampanja: Ciljane reklame putem Google Ads-a, društvenih mreža ili specijalizovanih blokčejn portala mogu privući pažnju potencijalnih korisnika i investitora, povećavajući vidljivost DApp-a u relevantnim krugovima.

Analiza performansi sistema

Praćenje performansi decentralizovanih aplikacija i njihovog uticaja na poslovne efekte može se izvršiti na sledeće načine:

- Analitika korisničkog angažovanja: Korišćenjem alata za analitiku (npr. Google Analytics, Dune Analytics za blokčejn specifične podatke) mogu se pratiti podaci kao što su broj korisnika, stopa zadržavanja, frekvencija korišćenja i geografska lokacija korisnika. Ovi podaci pomažu u razumevanju koliko su korisnici angažovani i koji su ključni segmenti publike.
- Praćenje transakcija: Analizom broja transakcija i učestalosti korišćenja pametnih ugovora može se oceniti kako DApp doprinosi poslovnim ciljevima, kao što su prihodi ili korisničko zadovoljstvo.
- Metode za ocenu poslovnih efekata: Postavljanje ključnih pokazatelja uspešnosti (KPI) kao što su smanjenje troškova, bolja efikasnost ili poboljšano korisničko iskustvo.

Razvoj decentralizovanih aplikacija



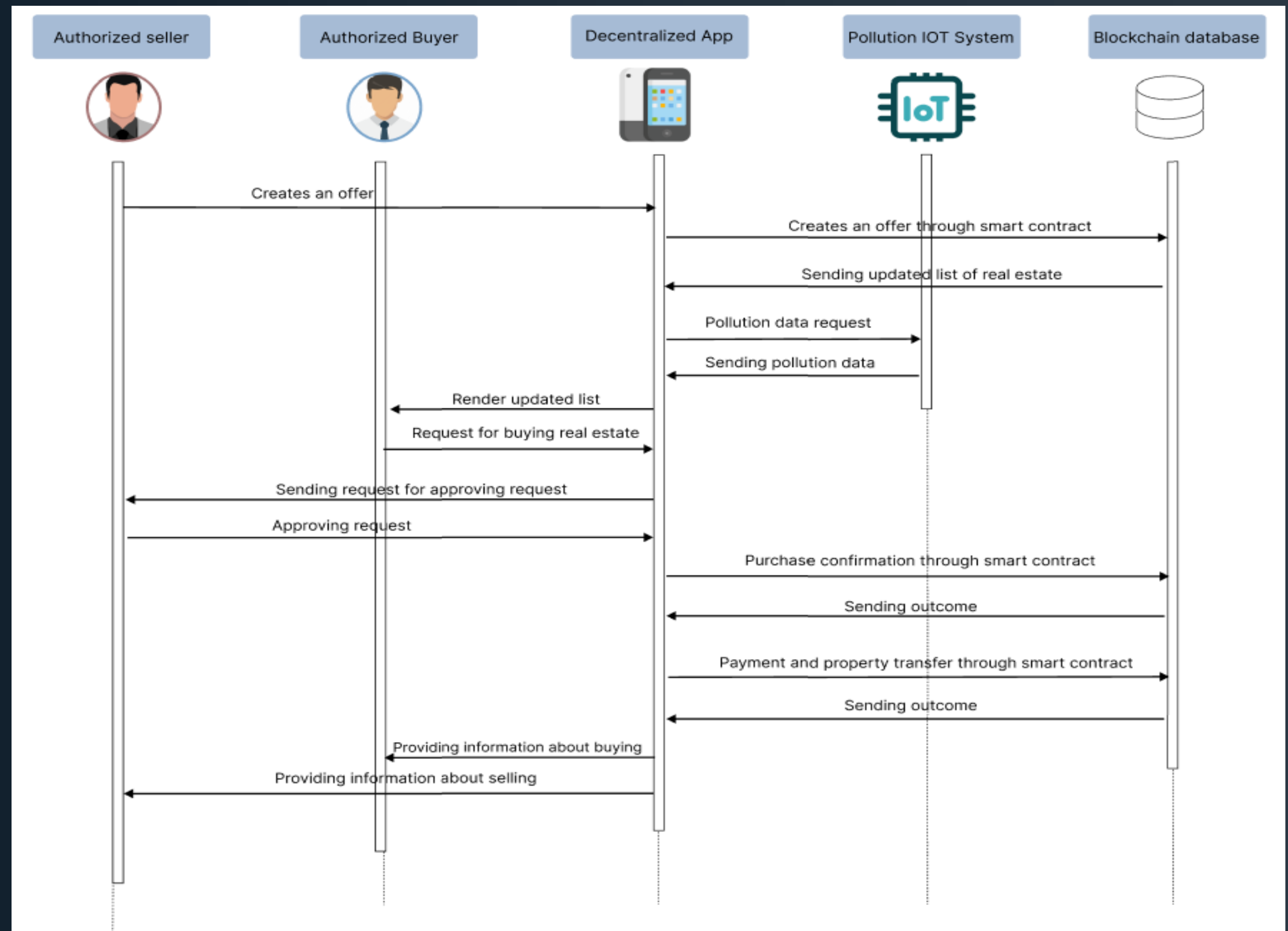
Razvoj Dapp za trgovinu nekretninama u pametnim gradovima

Projektni zahtev:

- Razviti decentralizovanu aplikaciju za trgovinu nekretninama u pametnim gradovima
- Razvijena DApp treba građanima da omogući:
 - Prikaz nekretnina po odabranim lokacijama
 - Praćenje zagađenja u realnom vremenu po lokacijama primenom inteligentnih uređaja
 - Informacije o nekretninama: kvadratura, vlasništvo, cena, lokacija, spratnost, itd.
 - Kupovinu ili plaćanje najma nekretnina putem pametnih ugovora i kripto valute.
- Korisnički interfejs treba da obezbedi jednostavnost korišćenja za sve učesnike u predloženom ekosistemu

Postupak razvoja decentralizovane aplikacije

- Korisnik (prodavac/kupac) se prijavljuje i interaguje sa sistemom.
- Prodavac kreira oglas koji se validira pametnim ugovorom.
- Aplikacija prikuplja podatke o zagađenju putem IoT sistema.
- Kupac šalje zahtev za kupovinu, što pokreće pametni ugovor za validaciju.
- Nakon odobrenja prodaje, pametni ugovor izvršava transfer vlasništva i sredstava.



Razvoj pametnih ugovora

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract RealEstate {
    address payable private beneficiary;
    uint256 private price;
    int256 private lat;
    int256 private lon;
    string private locationName;
    bool private registered;
    bool private mortgageFree;
    uint256 private sqft;
    string private floor;
    string private heatingType;
    uint256 private numberOfRooms;

    mapping(address => uint) pendingReturns;

    event RealEstateBought(address indexed buyer, uint256 price);
```

RealEstate.sol

- Predstavlja pojedinačne nekretnine u sistemu.
- Sadrži atribute, konstruktore, getere i funkciju za kupovinu.
- Upravljanje transakcijama vezanim za kupovinu nekretnina.

- Kreira i upravlja svim instancama nekretnina.
- Pruža centralni mehanizam za rukovanjem više nekretnina.
- Poboljšava skalabilnost i efikasno rukovanje aplikacijom.
- Generiše funkciju koja vraća prikaz svih postojećih nekretnina

RealEstateFactory.sol



```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

import "../RealEstate.sol";

contract RealEstateFactory {
    RealEstate[] public realEstates;

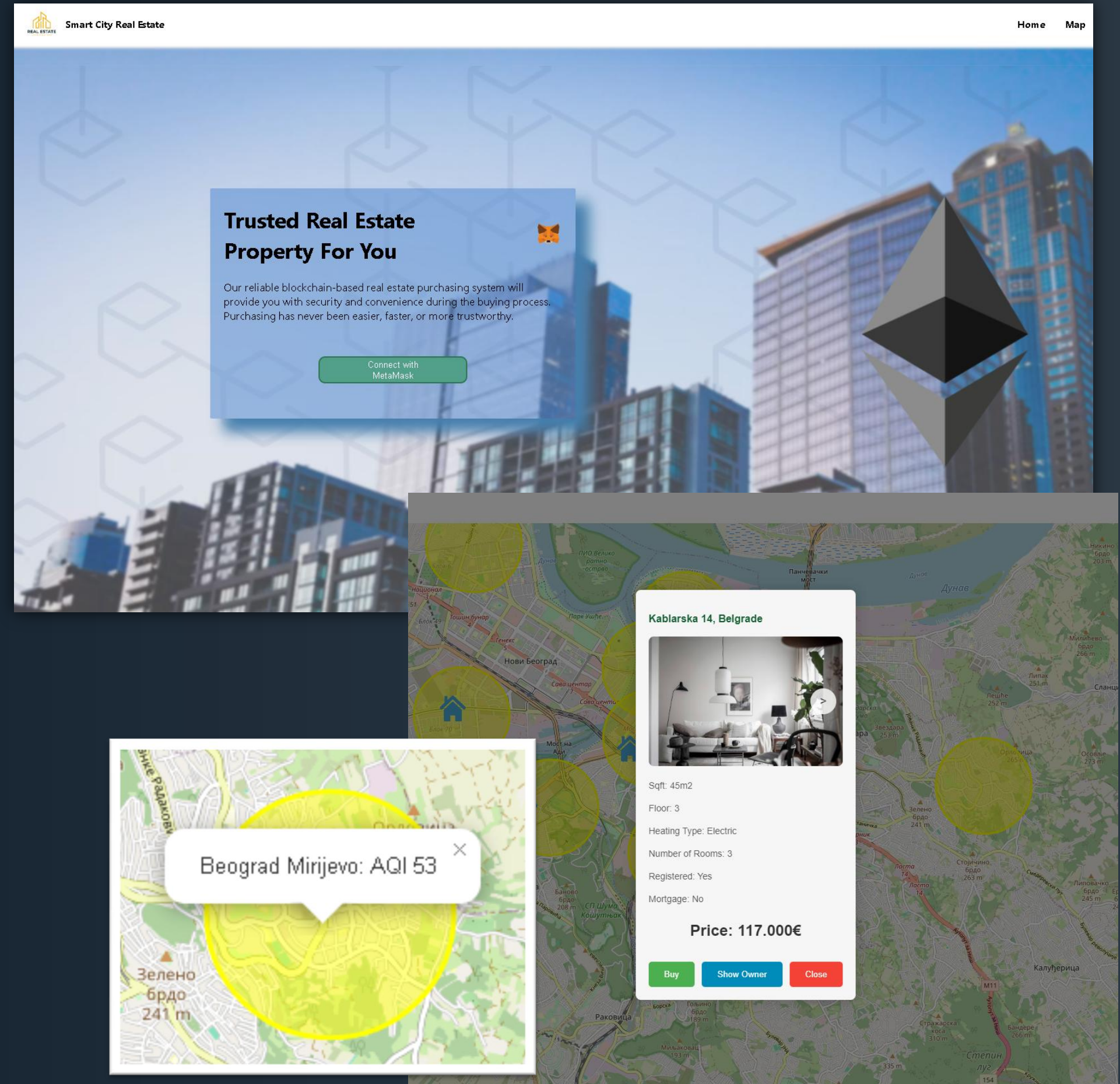
    function createRealEstate(address payable _beneficiary, uint256 _price, int256 _lat, int256 _lon,
        string memory _locationName, bool _registered, bool _mortgageFree, uint256 _sqft, string memory _floor,
        string memory _heatingType, uint256 _numberOfRooms) public {

        RealEstate newRealEstate = new RealEstate(_beneficiary, _price, _lat, _lon, _locationName,
            _registered, _mortgageFree, _sqft, _floor, _heatingType, _numberOfRooms);
        realEstates.push(newRealEstate);
    }

    function getAllRealEstates() public view returns (RealEstate[] memory) {
        return realEstates;
    }
}
```

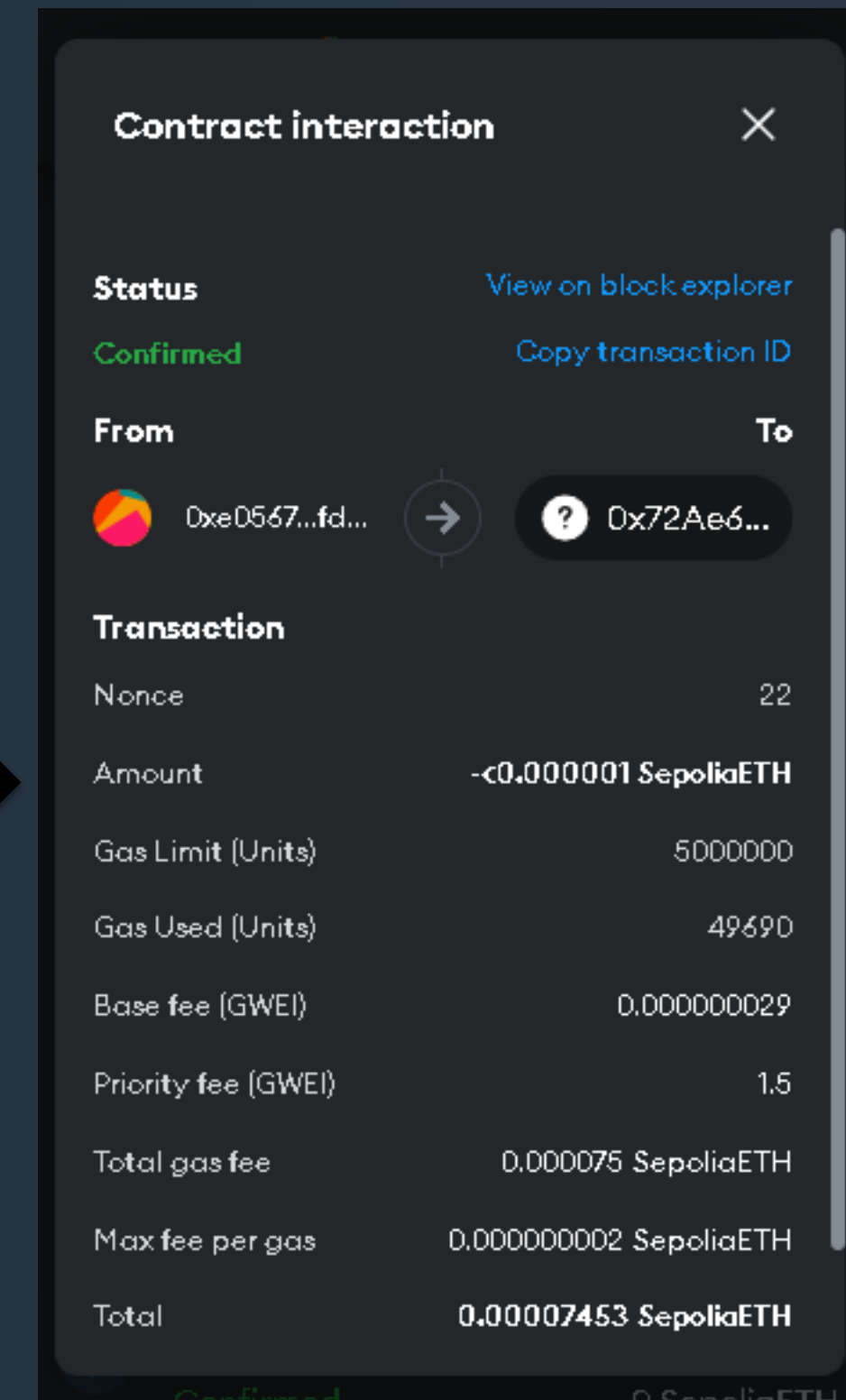
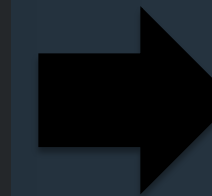
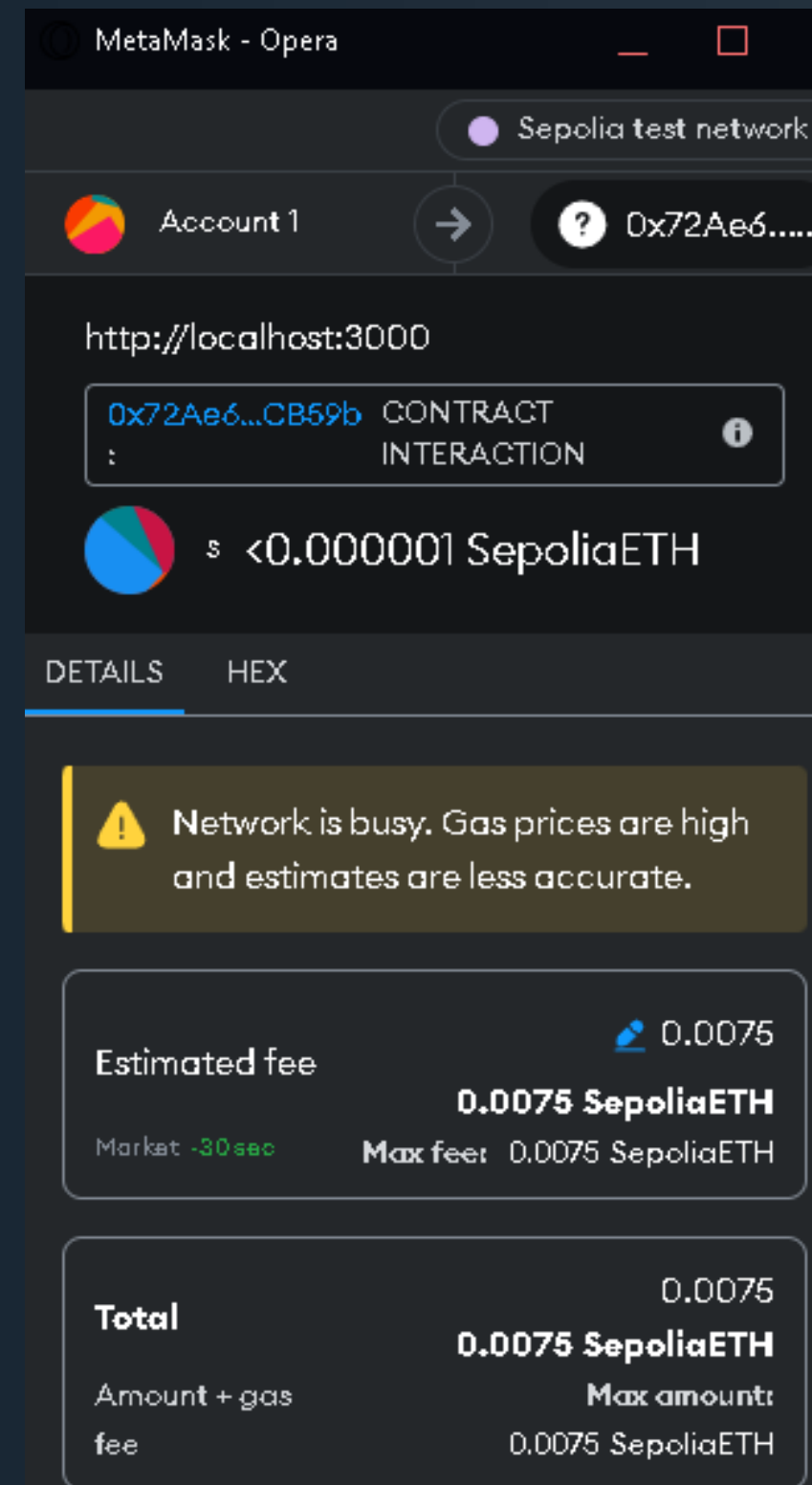
Razvoj front-end dela

- Tehnologija: Front-end deo aplikacije razvijen je korišćenjem React.js-a.
- Interaktivna mapa: Kreirana pomoću Leaflet React.js biblioteke, omogućava prikaz podataka o zagađenju i nekretninama.
- Geolokacija korisnika: Koristi se geolokacioni servis pretraživača za prikaz trenutne lokacije korisnika na mapi.
- Interakcija sa nekretninama: Korisnici mogu kliknuti na ikone kuća na mapi da bi dobili detaljne informacije o nekretninama.
- Vizuelni elementi: Prikazani su detalji kao što su cena, površina, broj soba i sl.



Izvršavanje transakcije za trgovinu nekretninama

- **MetaMask digitalni novčanik:**
Koristi se za pristup aplikaciji i izvršavanje transakcija za kupovinu nekretnina.
- **Pristup aplikaciji:** Korisnici se povezuju sa MetaMask-om i potvrđuju pristup aplikaciji radi korišćenja funkcionalnosti.
- **Izvršavanje transakcije:** Nakon što korisnik odabere nekretninu, MetaMask se koristi za iniciranje i potvrđivanje transakcije.
- **Potvrda kupovine:** Nakon uspešne validacije, nekretnina se registruje na ime kupca, a transakcija se završava kroz pametni ugovor.



Testiranje Dapp-a

- Sepolia test mreža: Transakcije se testiraju na Sepolia mreži radi simulacije stvarnih scenarija u kontrolisanom okruženju.
- Detaljan uvid u svaku transakciju, uključujući metodu koja se izvršava, nalog sa kojeg je transakcija poslata, kao i vrednost koja je prenet, omogućava transparentnost i praćenje svih aktivnosti tokom testiranja aplikacije.

↓ Latest 19 from a total of 19 transactions Download Page Data ▽

Transaction Hash	Method	Block	Age	From	To	Value	Txn Fee
0x8d7980921a...	Make Payment	5681979	29 secs ago	0x10c480Ae...332d5aDa8	OUT 0x767BBE8E...d01297C24	0 ETH	0.00007231
0x2119d79bf81...	0xa00f198a	5681976	1 min ago	0x10c480Ae...332d5aDa8	OUT 0x767BBE8E...d01297C24	0 ETH	0.00005656
0x37e46021ab...	Place Order	5681970	2 mins ago	0x10c480Ae...332d5aDa8	OUT 0x767BBE8E...d01297C24	0 ETH	0.00010897
0x5d142905f8a...	Place Order	5681960	4 mins ago	0x10c480Ae...332d5aDa8	OUT 0x767BBE8E...d01297C24	0 ETH	0.00003206
0x32a3ce4d51...	0x60806040	5681954	5 mins ago	0x10c480Ae...332d5aDa8	OUT Contract Creation	0 ETH	0.00219368
0xbe65045b12...	Place Order	5681905	15 mins ago	0x10c480Ae...332d5aDa8	OUT 0x259FbC44...815F45A46	0 ETH	0.00010897
0x5fcd504c366...	0x60806040	5681896	17 mins ago	0x10c480Ae...332d5aDa8	OUT Contract Creation	0 ETH	0.00219379

Zaključak



Zaključak – prednosti primene blokčejna

Blokčejn tehnologija predstavlja važan pravac digitalne transformacije jer omogućava sigurnu, transparentnu i pouzdanu razmenu podataka i transakcija bez potrebe za centralnim posrednikom.

Njena najveća vrednost ogleda se u tome što omogućava:

- veću transparentnost poslovnih procesa,
- sledljivost podataka, proizvoda i transakcija,
- smanjenje mogućnosti manipulacije i prevara,
- automatizaciju procesa kroz pametne ugovore,
- jačanje poverenja između učesnika u sistemu.

Zbog toga blokčejn ima veliki potencijal u oblastima kao što su finansije, e-trgovina, zdravstvo, obrazovanje, javna uprava, industrija i pametni gradovi.

Zaključak – trenutna ograničenja i pravci razvoja

Iako blokčejn nudi brojne prednosti, njegova šira primena i dalje zavisi od rešavanja određenih izazova. Najvažnija ograničenja odnose se na nedovoljno razvijenu regulativu, pravnu sigurnost, interoperabilnost između različitih sistema, kao i pitanja skalabilnosti i performansi.

Posebno je važno da se razviju jasni pravni okviri koji će omogućiti sigurnu primenu blokčejna ne samo u finansijskom sektoru, već i u drugim oblastima poslovanja i društva.

U budućnosti se očekuje veća integracija blokčejna sa emerging tehnologijama kao što su veštačka inteligencija, Internet inteligentnih uređaja, Big Data i cloud computing. Na taj način blokčejn može postati osnova za razvoj sigurnijih, pametnijih i efikasnijih digitalnih sistema.

UVOD U BLOKČEJN

Prof. dr Aleksandra Labus

aleksandra.labus@matf.bg.ac.rs

aleksandra.labus@fon.bg.ac.rs