



UNIVERZITET U NOVIM SADU,
PRIRODNO-MATEMATIČKI FAKULTET

Istraživački rad

Tema:

TOKENI ZA FINANSIRANJE

Profesor:

Prof. dr Vladimir Kurbalija

Student:

Nikola Veselinović 53m/24

Beograd, septembar 2025. godine

Sadržaj

Finansiski tokeni	2
Pametni ugovor (smart contract).....	3
Praktičan primer – Limunada Token.....	3
Tehnički infrastruktura	8
Plan implementacije.....	12
Beli papir.....	14
Obrazac za beli papir	14
Iznošenje investicionog tokena na evropsko tržište (EU) – regulatorni i operativni plan	16
Reference	17

Finansijski tokeni

Finansijski tokeni su **digitalni zapisi vrednosti na blokčejnu** koji predstavljaju neki oblik ulaganja ili finansijskog proizvoda. Oni mogu da funkcionišu slično kao hartije od vrednosti (npr. obveznice ili akcije), jer se izdaju u zamenu za novac i nosiocima donose određena prava – kao što su pravo na prinos (kamatnu stopu), pravo na otkup ili učešće u investicionom indeksu.

U Srbiji, po **Zakonu o digitalnoj imovini (2021)**, digitalni tokeni spadaju u kategoriju digitalne imovine, a njihovo izdavanje, kupovina i trgovina su zakonski regulisani. Postoje **dva osnovna tipa**:

1. **Virtuelne valute** (npr. Bitcoin, Ether) – služe uglavnom za plaćanje i razmenu.
2. **Digitalni tokeni** (npr. Finspot FIN, Virtus vinski token) – predstavljaju pravo investitora prema izdavaocu i često su povezani sa realnim finansijskim ili robnim proizvodima.

Kompanije izdaju finansijske tokene iz nekoliko razloga:

- **Prikupljanje kapitala** – Tokenizacija omogućava brže i fleksibilnije prikupljanje sredstava od investitora nego kroz bankarske kredite ili emisiju obveznica.
- **Demokratizacija ulaganja** – Tokeni se često emituju u manjim nominalama (npr. 1.000 RSD), što omogućava i malim investitorima da učestvuju.
- **Likvidnost i transparentnost** – Zahvaljujući blokčejnu, sve transakcije su javno zabeležene i lakše je pratiti vlasništvo i promet.
- **Inovativni investicioni proizvodi** – Tokene je moguće vezati za različite indekse, kamate, robu (vino, poljoprivredni proizvodi) ili čak poslovne projekte, pa otvaraju nove mogućnosti za finansiranje.

Investitori kupuju finansijske tokene jer oni nude:

- **Prinos (kamatni ili profit)** – Kod Finspot FIN/FIN2/FIN3 tokena, investitor oročava tokene u indeks i dobija kamatu od ~5–10% godišnje posle poreza.
- **Sigurnost i regulaciju** – U Srbiji emisije moraju biti usklađene sa Zakonom o digitalnoj imovini i često dobijaju odobrenje Komisije za hartije od vrednosti, slično prospektu kod akcija/obveznica.
- **Fleksibilnost** – Token se može prodati natrag izdavaocu ili preneti drugom licu. Kod nekih projekata (npr. Virtus vinski token), token se može zameniti i za realni proizvod, bocu vina.
- **Diversifikaciju portfolija** – Investitori dobijaju priliku da ulože u nove sektore (finansiranje faktoringa, poljoprivreda, vinarstvo) bez potrebe za direktnim ulaskom u biznis.

Kompanije koje izdaju digitalne tokene u Srbiji		
Kompanija	Token / Projekat	Opis / Status
Finspot d.o.o. (Beograd)	Finspot Faktoring Token: FIN, FIN2 i FIN3	Prva srpska kompanija koja je zvanično odobrena od strane Komisije za hartije od vrednosti da emituje digitalne tokene. finspot.rs/

Vinarija Virtus doo Žabari, Viteževo	Virtus Vinski Token	Vinarija koja je pripremila i objavila beli papir za digitalni token povezan sa vinom. klub.vinarijavirtus.rs
AVR Solar Park d.o.o. (Beograd)	AVR Solar Token	Finansiran projekat izgradnje solarene elektrane kroz prodaju digitalnih tokena. avrsolar.com
SunCarlito Beta	Solar Token ST_1	Kompanija koja je najavila model finansiranja putem digitalnog tokena za izgradnju solarne elektrane. suncarlitosolar.rs
The Walnut Enterprise	The Walnut Enterprise token: TWE_R , TWE_L , TWE_L2	Projekat u poljoprivredi (uzgajanje oraha) koji ima beli papir, sa izdavanjem digitalnih tokena. thewalnutfund.com
Treesury d.o.o. Beograd	Treesury Token	Projekat u poljoprivredi (uzgajanje lešnika i borovnica) koji ima beli papir, sa izdavanjem digitalnih tokena. treesury.com

Svi odobreni beli papiri se mogu naći na [sajtu Komisije za hartije od vrednosti](#).

Pametni ugovor (smart contract)

Pametni ugovor (smart contract) je **programski kod na blockchain mreži** koji automatski izvršava unapred definisana pravila i uslove, bez potrebe za posrednikom. Radi kao “**digitalni ugovor**”, jednom kada je postavljen na blockchain, uslovi su transparentni i ne mogu se menjati bez saglasnosti. Najčešće se koristi na mrežama poput **Ethereum-a, Solane ili Polygona**. Kod sadrži logiku npr. “*Ako investitor uloži X tokena do datuma Y → automatski mu pripada pravo na kamatu Z*”. Prednosti ovakvih tipova ugovora su: automatizacija, smanjenje troškova, transparentnost i nemogućnost manipulacije nakon objave.

Investicioni tokeni se izdaju i funkcionišu putem pametnih ugovora. Na primer: Finspot FIN3 token je kreiran na blockchainu kroz pametni ugovor koji definiše pravila o kupovini, oročavanju i otkupu. Dakle pametni ugovor je “tehnologija”, a investicioni token je “proizvod” koji se na toj tehnologiji zasniva.

Praktičan primer – Limunada Token

Primer pametnog ugovora za Ethereum koji ilustruje investicioni token “**Limunada Token**” (LWT_1) sa **30-dnevnim ciklusom** i **podelom profita 50/50**. Primer koristi stabilni ERC-20 token kao valutu uplate/isplate i OpenZeppelin biblioteke radi bezbednosti.

Model (pojednostavljen):

- Uplata po tokenu = **trošak proizvodnje** (za potrebe ovog primera 100 din).
- Po isteku 30 dana, *otkupna isplata* po tokenu = **trošak + 50% marže** (gde je marža = prodajna cena - trošak).
- Izdavalac mora **pre isteka** da u ugovor **uplati prihod** (u ovom primeru od prodaje limunade) kako bi bilo dovoljno sredstava za otkup.
- Ugovor blokira transfer LWT_1 (ne-tradabilan tokom ciklusa) i dozvoljava **otkup (redeem)** nakon unlockTime.

Kod je napisan u **Solidity-ju**, glavnom programskom jeziku za pametne ugovore na **Ethereum-u** (i EVM-kompatibilnim mrežama kao što su Polygon, Binance Smart Chain, Avalanche, Optimism, Arbitrum itd.). Ukratko o Solidity-ju: sintaksa liči na **JavaScript** i **C++**, ali je specijalizovan za rad sa blockchainom, radi u kontekstu Ethereum Virtual Machine (**EVM**) i koristi se za kreiranje i upravljanje **pametnim ugovorima**, ERC-20 tokenima, NFT-ovima i DeFi protokolima.

```

1. // SPDX-License-Identifier: MIT
2. pragma solidity ^0.8.24;
3.
4. /**
5.  * LWT_1 (Limunada Token) – investicioni ERC-20 sa:
6.  * - KYC/whitelist (COMPLIANCE_ROLE upravlja dozvoljenim adresama),
7.  * - 30-dnevnim lock-om (zabrana transfera do unlockTime),
8.  * - fiksnim otkupom (redeem) = costPerToken + 50% marže,
9.  * - uplata/isplata u stablecoinu (currency, npr. USDC/DAI),
10. * - RBAC: DEFAULT_ADMIN_ROLE, MINTER_ROLE, TREASURER_ROLE, PAUSER_ROLE, COMPLIANCE_ROLE,
11. * - pause/unpause, batch whitelist, reentrancy zaštita.
12. *
13. * Pre produkcije: audit, pravna usklađenost, testovi,..
14. */
15.
16. import "@openzeppelin/contracts/token/ERC20/extensions/ERC20Burnable.sol";
17. import "@openzeppelin/contracts/token/ERC20/IERC20.sol";
18. import "@openzeppelin/contracts/token/ERC20/extensions/IERC20Metadata.sol";
19. import "@openzeppelin/contracts/security/ReentrancyGuard.sol";
20. import "@openzeppelin/contracts/access/AccessControl.sol";
21. import "@openzeppelin/contracts/utils/Pausable.sol";
22.
23. contract LWT1 is ERC20Burnable, Pausable, AccessControl, ReentrancyGuard {
24.     // ===== Roles =====
25.     bytes32 public constant MINTER_ROLE = keccak256("MINTER_ROLE"); // emisija LWT_1
26.     bytes32 public constant TREASURER_ROLE = keccak256("TREASURER_ROLE"); // povlačenje cost-
a, dopuna prihoda
27.     bytes32 public constant PAUSER_ROLE = keccak256("PAUSER_ROLE"); // pauza
28.     bytes32 public constant COMPLIANCE_ROLE = keccak256("COMPLIANCE_ROLE"); // whitelist
upravljanje
29.
30.     // ===== Eksterna valuta za uplate/isplate (npr. USDC/DAI) =====
31.     IERC20 public immutable currency;
32.     uint8 public immutable currencyDecimals;
33.
34.     // ===== Takt investicije =====
35.     uint256 public immutable startTime; // početak ciklusa
36.     uint256 public immutable unlockTime; // startTime + 30 dana
37.     uint256 public subscriptionEnd; // do kada je dozvoljena kupovina (mint)
38.
39.     // ===== Ekonomika =====
40.     uint256 public costPerToken; // npr. 100 (u "currency" decimalama)
41.     uint256 public salePricePerUnit; // npr. 200 (u "currency" decimalama)
42.
43.     // Beležimo koliko je osnove (cost) prikupljeno – za kontrolisano povlačenje
44.     uint256 public totalCollectedCost;

```

```

45.
46. // ===== Compliance (KYC whitelist) =====
47. mapping(address => bool) public isWhitelisted;
48.
49. // ===== Događaji =====
50. event Purchased(address indexed investor, uint256 amount, uint256 paid);
51. event Redeemed(address indexed investor, uint256 amount, uint256 payout);
52. event OwnerWithdrawCost(uint256 amount);
53. event OwnerFundedRevenue(uint256 amount);
54. event EconomicsUpdated(uint256 costPerToken, uint256 salePricePerUnit);
55. event WhitelistUpdated(address indexed account, bool allowed);
56. event WhitelistBatchUpdated(uint256 count, bool allowed);
57.
58. // ===== Konstruktor =====
59. constructor(
60.     address _admin,
61.     address _currency,
62.     string memory _name,
63.     string memory _symbol,
64.     uint256 _startTime,
65.     uint256 _subscriptionEnd,
66.     uint256 _costPerToken,
67.     uint256 _salePricePerUnit
68. ) ERC20(_name, _symbol) {
69.     require(_admin != address(0), "admin=0");
70.     require(_currency != address(0), "currency=0");
71.     require(_startTime >= block.timestamp, "start in past");
72.     require(_subscriptionEnd >= _startTime, "bad subscriptionEnd");
73.     require(_salePricePerUnit >= _costPerToken, "sale < cost");
74.
75.     _grantRole(DEFAULT_ADMIN_ROLE, _admin);
76.     _grantRole(MINTER_ROLE, _admin);
77.     _grantRole(TREASURER_ROLE, _admin);
78.     _grantRole(PAUSER_ROLE, _admin);
79.     _grantRole(COMPLIANCE_ROLE, _admin);
80.
81.     currency = IERC20(_currency);
82.     currencyDecimals = IERC20Metadata(_currency).decimals();
83.
84.     startTime = _startTime;
85.     unlockTime = _startTime + 30 days;
86.     subscriptionEnd = _subscriptionEnd;
87.
88.     costPerToken = _costPerToken;
89.     salePricePerUnit = _salePricePerUnit;
90. }
91.
92. // ===== Pogodnosti/ograničenja transfera (lock + whitelist) =====
93. function _update(address from, address to, uint256 value) internal override whenNotPaused {
94.     // Dozvoliti mint (from=0) i burn (to=0) bez dodatnih ograničenja.
95.     if (from != address(0) && to != address(0)) {
96.         // 1) Lock do roka dospeća
97.         require(block.timestamp >= unlockTime, "Transfers locked until unlock");
98.
99.         // 2) KYC/whitelist na obe strane
100.        require(isWhitelisted[from] && isWhitelisted[to], "Transfer not allowed (KYC)");
101.    }
102.    super._update(from, to, value);
103. }
104.
105. // ===== Ekonomika =====
106. function profitSharePerToken() public view returns (uint256) {
107.     // 50% marže: (sale - cost)/2
108.     return (salePricePerUnit - costPerToken) / 2;
109. }

```

```

110.
111.     function payoutPerToken() public view returns (uint256) {
112.         // isplata pri otkupu = cost + 50% marže
113.         return costPerToken + profitSharePerToken();
114.     }
115.
116.     // Do startTime je dozvoljeno prilagoditi ekonomiku (ako treba)
117.     function adminUpdateEconomics(uint256 _cost, uint256 _sale)
118.         external
119.         onlyRole(DEFAULT_ADMIN_ROLE)
120.     {
121.         require(block.timestamp < startTime, "Cycle started");
122.         require(_sale >= _cost, "sale < cost");
123.         costPerToken = _cost;
124.         salePricePerUnit = _sale;
125.         emit EconomicsUpdated(_cost, _sale);
126.     }
127.
128.     // Opciona korekcija subscriptionEnd (npr. produženje tokom pre-sale)
129.     function adminSetSubscriptionEnd(uint256 _subscriptionEnd)
130.         external
131.         onlyRole(DEFAULT_ADMIN_ROLE)
132.     {
133.         require(_subscriptionEnd >= startTime, "bad subscriptionEnd");
134.         subscriptionEnd = _subscriptionEnd;
135.     }
136.
137.     // ===== Kupovina (pretplata) =====
138.     /**
139.      * @dev Kupovina se modeluje mint-ovanjem LWT_1 nakon uplate "cost" u stablecoinu.
140.      * Potrebno je prethodno odobriti (approve) transfer na ovaj ugovor.
141.      */
142.     function buy(uint256 amount)
143.         external
144.         nonReentrant
145.         whenNotPaused
146.         onlyWhitelisted(msg.sender)
147.     {
148.         require(amount > 0, "amount=0");
149.         require(block.timestamp <= subscriptionEnd, "Subscription ended");
150.
151.         uint256 totalCost = amount * costPerToken;
152.         require(currency.transferFrom(msg.sender, address(this), totalCost), "transferFrom
153.         failed");
154.
155.         totalCollectedCost += totalCost;
156.         _mint(msg.sender, amount);
157.
158.         emit Purchased(msg.sender, amount, totalCost);
159.     }
160.
161.     // ===== Trezor operacije (off-chain poslovanje) =====
162.     // Povlačenje prikupljene "osnove" (trošak proizvodnje) ka izdavaocu za finansiranje
163.     // proizvodnje
164.     function treasurerWithdrawCollectedCost(uint256 amount)
165.         external
166.         nonReentrant
167.         onlyRole(TREASURER_ROLE)
168.     {
169.         require(amount <= totalCollectedCost, "exceeds collected cost");
170.         totalCollectedCost -= amount;
171.         require(currency.transfer(msg.sender, amount), "transfer failed");
172.         emit OwnerWithdrawCost(amount);
173.     }

```

```

173.
174. // Vraćanje prihoda od prodaje u ugovor – da bi bilo dovoljno sredstava za otkup/redeem
175. function treasurerFundRevenue(uint256 amount)
176.     external
177.     nonReentrant
178.     onlyRole(TREASURER_ROLE)
179. {
180.     require(amount > 0, "amount=0");
181.     require(currency.transferFrom(msg.sender, address(this), amount), "fund transfer
failed");
182.     emit OwnerFundedRevenue(amount);
183. }
184.
185. // ===== Otkup (redeem) =====
186. function redeem(uint256 amount)
187.     external
188.     nonReentrant
189.     whenNotPaused
190.     onlyWhitelisted(msg.sender)
191. {
192.     require(block.timestamp >= unlockTime, "Not unlocked");
193.     require(amount > 0, "amount=0");
194.     require(balanceOf(msg.sender) >= amount, "insufficient LWT_1");
195.
196.     uint256 perToken = payoutPerToken();
197.     uint256 totalPayout = amount * perToken;
198.
199.     require(currency.balanceOf(address(this)) >= totalPayout, "insufficient contract
funds");
200.
201.     _burn(msg.sender, amount);
202.     require(currency.transfer(msg.sender, totalPayout), "payout transfer failed");
203.
204.     emit Redeemed(msg.sender, amount, totalPayout);
205. }
206.
207. // ===== Compliance / Whitelist =====
208. modifier onlyWhitelisted(address account) {
209.     require(isWhitelisted[account], "Not whitelisted");
210.     _;
211. }
212.
213. function setWhitelisted(address account, bool allowed)
214.     external
215.     onlyRole(COMPLIANCE_ROLE)
216. {
217.     isWhitelisted[account] = allowed;
218.     emit WhitelistUpdated(account, allowed);
219. }
220.
221. function setWhitelistedBatch(address[] calldata accounts, bool allowed)
222.     external
223.     onlyRole(COMPLIANCE_ROLE)
224. {
225.     for (uint256 i = 0; i < accounts.length; i++) {
226.         isWhitelisted[accounts[i]] = allowed;
227.     }
228.     emit WhitelistBatchUpdated(accounts.length, allowed);
229. }
230.
231. // ===== Pause =====
232. function pause() external onlyRole(PAUSER_ROLE) { _pause(); }
233. function unpause() external onlyRole(PAUSER_ROLE) { _unpause(); }
234. }

```


Životni ciklus Limunada Tokena (LWT_1) - 30 dana



Tehnički infrastruktura

Za izradu tokena za finansiranje potrebno je izabrati blockchain mrežu, izabrati standard, implementirati pametni ugovor, integrisati sistem sa bankarskim (fiat) sistemom, implementirati mere bezbednosti i kontrole sistema, kao i platforme (npr. veb stranice) za izvršavanje transakcija.

Kod izbora blockchain mreže možemo koristiti **javne EVM mreže** (Ethereum mainnet, Polygon), prednost u interoperabilnosti i dostupnosti DeFi ekosistema, **alternativne mreže (Solana)**, pogodne za NFT/SPL modele sa nižim troškovima transakcija, ili **privatne mreže**, u slučaju potrebe za većom kontrolom i zatvorenim ekosistemom. Izbor mreže zavisi od poslovnog modela i regulatornih ograničenja, međutim, zbog jednostavnog pristupa ERC-20 standardu i integracije sa postojećim alatima, **Polygon** predstavlja praktičnu polaznu tačku za LWT_1.

Zavisno od izbora mreže dostupni su sledeći standardi.

EVM (Ethereum & kompatibilne mreže – npr. Polygon)

- **ERC-20 (EIP-20)** – fungibilni tokeni (sve jedinice jednake). To je osnovni standard kod DeFi-ja: transfer, approve, transferFrom, događaji Transfer/Approval. Interoperabilnost sa wallet-ima, brzama i protokolima je razlog njegove dominacije.
- **ERC-4626 (Tokenized Vault Standard)** – standardizuje “kasu/vault” za prinose (shares naspram jednog ERC-20 underlying-a). Koristi se kad je prinos on-chain i akumulira se kroz exchange-rate.
- **ERC-1400 (security token)** – skup specifikacija za regulisane (vrednosne) tokene: kontrola transfera, operatori, dokumenti, greške, delimično-fungibilni 1410 itd. Koristi se kada treba stroža usaglašenost i “permissioned” tok.
- **ERC-3643 (ex T-REX)** – permissioned tokeni sa ugrađenim identitetom (ONCHAINID) i pravilima pristupa vlasništvu; često se koristi za RWA.

- dopune koje se često dodaju ERC-20-u: **EIP-2612 Permit** za potpisno odobrenje bez gas-a; **ERC-2981** za royalty kod NFT/1155 ali nisu obavezne ovde

Solana ekosistem

- **SPL Token Program** – ekvivalent ERC-20/721 u Solana svetu (fungibilni i ne-fungibilni tokeni).
- **Metaplex Token Metadata** – standard za metapodatke (i za fungibilne i za NFT); industrijski standard na Solani.

U Srbiji koriste se sledeće mreže i standardi:

- **Finspot – FIN / FIN2 / FIN3: ERC-20 na Polygon-u (OpenZeppelin)**, sa KYC/whitelist “compliance hook-om” i integracijom investicionih proizvoda/rokova.
- **The Walnut Enterprise – TWE_R / TWE_L / TWE_L2: ERC-20 na Polygon-u**, sa ograničenim transferima (samo izdavalac↔investitor ili whitelisted investitor).
- **Virtus vinski token: Solana SPL + Metaplex (NFT)** – svaki token predstavlja jednu bocu (jedinstveno pravo).

Za naš primer LWT_1 preporučuje se **ERC-20 na Polygon-u** (zbog niskog troška i jake interoperabilnosti). Za model prinosa može se koristiti jednostavni **lock/escrow** sa rokom (maturityTimestamp) i **redeem** isplatom po fiksnoj formuli – baš kao u tvom LWT_1 opisu. (Ako bi prinos bio on-chain i promenljiv, razmotrio bi se **ERC-4626**, ali kod tebe profit dolazi iz off-chain prodaje.). Zarad bezbednosti i usaglašenosti trebalo bi dodati **compliance hook** (whitelist KYC), ograničenja transfera do dospeća, i/ili razmotriti **ERC-1400 / ERC-3643** ako regulator/poslovni model traže eksplicitno permissioned tok i detaljnu kontrolu prenosa.

Kako metodički izabrati standard

1. Priroda prava

- Sve jedinice identične → **ERC-20**.
- Svaka jedinica predstavlja specifično dobro/pravo → **NFT (ERC-721/1155)** ili **SPL+Metaplex** na Solani.

2. Regulatorni režim i KYC

- Potreban permissioned tok (ograničenja kome se šalje, “investor eligibility”) → **ERC-1400** ili **ERC-3643** (ili ERC-20 + sopstveni compliance hook).

3. Mehanika prinosa

- **Fiksni, off-chain profit** sa otkupom na dan 30 → **ERC-20 + lock/escrow + redeem** (kao u LWT_1).
- **On-chain, promenljiv prinos** → **ERC-4626** (shares + exchange rate).

4. Lanac & trošak

- EVM mreže (npr. **Polygon**) su praktično-standard za ERC-20 u domaćoj praksi.

5. Operativna usklađenost

- RBAC + multisig, pause/upgrade, snapshot ako treba “record date”. (preporučeno i u lokalnim materijalima)

„Fiat“ novac je **državno izdata valuta** (npr. RSD) koja **nije pokrivena** zlatom ili drugom robom; vrednost joj proizilazi iz **zakonskog statusa, ponude/potražnje i poverenja** u izdavaoca (državu/centralnu banku). To je suprotnost „komoditetnom“ novcu (zlatnik, srebro) i različito je od „reprezentativnog“ novca (vaučer zamenljiv za robu). Danas su skoro sve velike valute fiat.

„Fiat sistem“ u praksi znači: **centralna banka + banke/platne institucije + platna infrastruktura** (kartice, nalog za prenos, instant plaćanja). U Srbiji to uključuje i **IPS** sistem Narodne banke Srbije za **instant plaćanja u sekundama** (za pojedinačne iznose do RSD 300.000).

Kako povezati LWT_1 sa fiat sistemom (RSD)? Moramo konsultovati regulativni okvir pre tehničke integracije. **Zakon o digitalnoj imovini** propisuje da pružanje usluga na tržištu digitalne imovine u Srbiji zahteva **licencu** (NBS – virtuelne valute; KHOV – digitalni tokeni). Nedoovoljeno pružanje je protivzakonito. **Zakon o platnim uslugama** odnosi se na platne institucije i pružanje/oglašavanje platnih usluga, informisanje korisnika, zaštitu potrošača, itd. Ako ne želimo sami da podnosimo za licencu, možemo da radimo preko **licenciranog PSP-a** (payment service provider). Ukratko: za „fiat on-ramp/off-ramp“ koristite se banke/PSP (RSD ↔ stablecoin) i licencirani DASP (pružaoca usluga u digitalnoj imovini) u skladu sa zakonom o digitalnoj imovini.

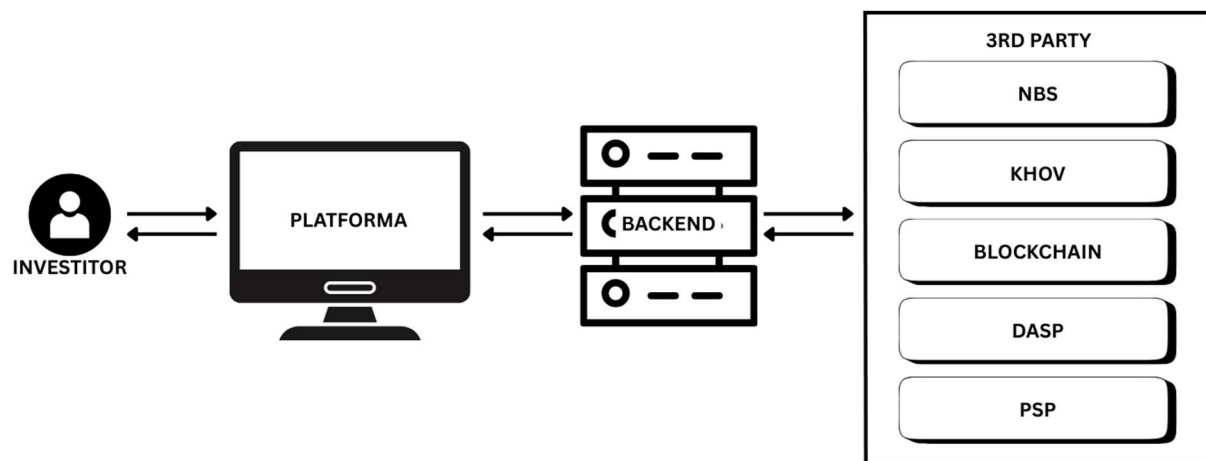
Ulaz novca (on-ramp RSD → on-chain)

1. **Onboarding investitora (KYC/AML)** u vašoj platformi.
2. Investitor bira način uplate **u RSD**:
 - **IPS transfer** (instant, QR kod u aplikaciji) – preporučeno do 300k RSD po nalogu.
 - Klasičan prenos / kartično plaćanje (preko PSP-a).
3. **PSP/banka** izvrši naplatu i šalje **webhook/izvod** vašem backend-u.

- Backend radi **reconciliaciju** (referenca uplate ↔ korisnički nalog), zatim konvertuje RSD u **stablecoin** (npr. USDC/DAI) preko **licenciranog DASP-a**.
- Treasury šalje stablecoin u **LWT_1 pametni ugovor**, koji **mintuje** LWT_1 investitoru (ili vi mintujete pa investitor polaže stablecoin u ugovor – zavisi od modela).

Izlaz novca (off-ramp on-chain → RSD)

- Po isteku 30 dana investitor poziva **redeem()** na LWT_1; ugovor obračuna iznos.
- Stablecoin iz ugovora ide u vaš **trezor**; preko licenciranog DASP-a se menja u **RSD**.
- Isplata investitoru u RSD:**
 - Za iznose do 300k RSD po nalogu – **IPS** (novac je za par sekundi na računu).
 - Za veće iznose – standardni međubankarski prenos/RTGS preko banke/PSP-a.
- Backend zatvara **knjigovodstveni trag** (burn LWT_1, izvod banke, poreske evidencije).



Najčešći problemi:

- KYC/transfer restrikcije:** uvek radite proveru u hook-u pre transfera (ili koristite “restricted token” obrazac); držite whitelist **on-chain**, a sinkronizujte s back-endom.
- Kamata i zaokruživanje:** radite sa 18 decimala i testirajte “edge” slučajeve; preferirajte **pull-isplate** (claim) radi gas/DoS otpornosti.
- Ročnost:** posle maturity definišite jasnu semantiku (da li se transferi gase, da li je obavezan otkup ili samo omogućeni redeem).

Plan implementacije

1. **Osnova pametnog ugovora (token standard + zaštite)**
 - **Izbor standarda:** ERC-20 (LWT_1 je fungibilan).
 - **Biblioteke:** OpenZeppelin (ERC20, AccessControl, Pausable, ReentrancyGuard).
 - **Parametri:** costPerToken, salePricePerUnit, startTime, unlockTime.
 - **Artefakti:** kontrakt + ABI, migracije, README sa parametrima i adresama.
2. **Compliance hook + ročnost (maturity)**
 - **Whitelist (KYC):** pre-transfer provera subjekata (investitor mora biti na listi).
 - **Ročnost:** zabrana transfera do unlockTime; redeem() posle dospeća spaljuje tokene i isplaćuje $\text{cost} + (\text{sale} - \text{cost})/2$.
 - **Konfig:** batch-whitelisting, revokacija, audit log događaja.
3. **Modul prinosa (po potrebi)**
 - **Osnovni LWT_1:** "lock/escrow" (fiksna formula).
 - **Alternativa:** ERC-4626 (ako deo prinosa postane on-chain) ili **Merkle-claim** (ako se profit deli periodično, off-chain obračun → on-chain claim).
4. **Upravljanje i nadogradivost**
 - **RBAC:** DEFAULT_ADMIN_ROLE, MINTER_ROLE, TREASURER_ROLE, PAUSER_ROLE, COMPLIANCE_ROLE.
 - **Vlasništvo:** Safe (Gnosis) multisig drži administratorske role.
 - **(Opciono) Ugradiva nadogradnja:** UUPS + **timelock** na administrativne akcije.
5. **Testovi i kvalitet koda**
 - **Unit/integration/invariant/fuzz** testovi (Foundry/Hardhat).
 - **Static analysis:** Slither, MythX/Mythril; gas snapshot.
 - **Coverage $\geq 90\%$** ključne logike (mint, whitelist, redeem, pauza).
6. **CI/CD i reproduktivni buildovi**
 - **Pipelines:** lint + test + static analysis + build artefakti.
 - **Verifikacija na explorer-u** (Polygonscan/Etherscan); uporedna provera bytecode-a.
 - **Tagovanje release-a** sa parametrima deploy-a.
7. **Okruženja i migracije**

- **Dev/test:** lokalni anvil + testnet (Sepolia/Amoy).
 - **Mainnet/Polygon:** skripte za inicijalno podešavanje rola, whitelista, limita.
 - **Seeding:** demo investitori, “happy-path” scenario (buy → withdraw cost → fund revenue → redeem).
8. **Bezbednost (pre go-live “gate”)**
- **Interni security review + eksterni audit.**
 - **Runbook incidenta:** pauza ugovora, ograničenja rola, key management.
 - **Bounty (po želji)** i “kill-switch” samo kroz multisig.
9. **KYC/AML i regulatorna usklađenost**
- **Tok registracije:** verifikacija identiteta (KYC/KYB), PEP/sanctions screening, evidencije.
 - **Politike & procedure:** ograničenja, monitoring transakcija, čuvanje dokaza.
 - **Dokumentacija za odobrenje belog papira (KHOV)** i interne politike (privacy/DP, IT bezbednost).
10. **FIAT/RSD platna integracija**
- **PSP:** kartice + **IPS QR;** webhook-ovi/izvodi za reconciliaciju.
 - **Konverzija RSD↔stablecoin:** preko licenciranog DASP-a; trezor (multisig) vrši on-chain transfere.
 - **Isplate (redeem):** stablecoin → RSD → **IPS/RTGS** isplata investitoru; zatvaranje knjigovodstvenog traga.
11. **Back-office i operative**
- **Reconciliacija:** (bankovni izvod ↔ PSP webhook ↔ on-chain događaji).
 - **Knjigovodstvo i porezi:** evidencija otkupa, kapitalne dobiti/prihoda, PDV tretman po modelu.
 - **Izveštavanje:** periodični reporti, dnevni settlement, kontroling.
12. **UAT / pilot i lansiranje**
- **UAT plan:** test grupe investitora, limiti, failover scenariji (pauza, refund).
 - **Go-live checklist:** adresar rola, whiteliste, depozit prihoda, verifikacija koda, objava belog papira i adresa ugovora.
13. **Produkcija, monitoring i održavanje**
- **Nadzor:** alerti na salda (trezor/ugovor), greške webhook-a, neobične tokove.

- **Operativne promene:** dodavanje investitora, nove runde (novi startTime/unlockTime), izmene white-lista.
- **Compliance & regulatorni reporting:** čuvanje logova, objave izmena belog papira, usklađivanje sa zahtevima nadzora.

Beli papir

Beli papir (white paper) u kontekstu digitalne imovine je **sveobuhvatan dokument** koji izdavalac tokena priprema kako bi potencijalnim investitorima pružio ključne informacije o projektu. On je ekvivalent prospektu kod hartija od vrednosti. Sadrži opis izdavaoca, tehničke i pravne karakteristike tokena, prava i obaveze investitora, rizike, poreski tretman i plan upotrebe sredstava.

Praktično, beli papir služi da:

- **informiše investitore** o prirodi i ciljevima projekta,
- **objasni tokene** (tehnički aspekt, prava, obaveze, način upotrebe i otkupa),
- **predstavi rizike i zaštitne mehanizme**,
- **osigura transparentnost i poverenje** između izdavaoca i investitora,
- **ispuni regulatorne zahteve**, jer se bez odobrenog belog papira ICO ne može javno oglašavati u Srbiji

Prema Zakonu o digitalnoj imovini i smernicama regulatora, beli papir mora da obuhvatiti:

- **Podatke o izdavaocu** (pravna forma, sedište, APR registracija, tim, finansijski izveštaji),
- **Opis digitalne imovine** (token, blockchain mreža, pametni ugovor, broj i cena tokena),
- **Razloge i plan upotrebe sredstava** (biznis plan, projekcije, finansiranje),
- **Rizike** (tržišni, tehnološki, regulatorni, likvidnosni),
- **Poreski tretman** (PDV, porez na kapitalnu dobit fizičkih i pravnih lica),
- **Mere zaštite podataka i AML/KYC procedure**,
- **Odgovornost izdavaoca** i izjavu o tačnosti podataka.

U Srbiji beli papir i izdavanje digitalne imovine reguliše **Zakon o digitalnoj imovini** (Sl. glasnik RS br. 153/2020). Dva ključna regulatora su: **Komisija za hartije od vrednosti (KHOV)** nadležna za digitalne tokene i **Narodna banka Srbije (NBS)** nadležna za virtuelne valute.

Regulatori odobravaju objavljivanje belog papira i vrše **licenciranje i nadzor** nad izdavaocima i pružaocima usluga digitalne imovine. Beli papir **ne može biti javno objavljen niti ponuđen investitorima bez prethodnog odobrenja KHOV-a**.

Zašto je važan?

- **Za investitore:** pruža ključne informacije za donošenje odluke o ulaganju i upozorava na rizike.
- **Za izdavaoca:** osigurava pravnu usklađenost, omogućava javno oglašavanje tokena i povećava poverenje tržišta.
- **Za državu:** omogućava nadzor i sprečava zloupotrebe (npr. pranje novca, prevare).

Obrazac za beli papir

1. Reč izdavaoca tokena

Podaci o kompaniji (naziv, sedište, APR registracija, matični broj, osnivači, tim, licence).

2. Svrha belog papira

Objašnjenje svrhe dokumenta, ciljeva, regulatornog okvira i razloga izdavanja.

3. Skraćenice i definicije

Definicije pojmova: digitalni token, blokčejn, pametni ugovor, AML/KYC, itd.

4. Uvod / Opis projekta

Istorija firme, tržište, poslovni model i analiza industrije.

5. Razlozi za inicijalnu ponudu i namena sredstava

Detaljan plan korišćenja prikupljenih sredstava.

6. Token – karakteristike i prava

Naziv i oznaka tokena, blockchain mreža, broj tokena i cena, prava i obaveze imalaca, upotreba tokena.

7. Inicijalna ponuda tokena

Period i trajanje ponude, cena i način kupovine, kvalifikovana lica, KYC/KYB i AML postupci, način plaćanja.

8. Rizici

Tržišni, kreditni, likvidnosni, regulatorni i tehnološki rizici, kao i posebna upozorenja.

9. Poreski tretman

PDV, oporezivanje fizičkih i pravnih lica, kapitalna dobit.

10. Zaštita podataka o ličnosti

Rukovalac podacima, svrha i pravni osnov obrade, vrste podataka i period čuvanja, prava lica.

11. Sprečavanje pranja novca i finansiranja terorizma (AML)

KYC/KYB postupci, provera identiteta i porekla sredstava, usklađenost sa zakonima.

12. Dodatne informacije

Povezana lica, izjave odgovornih lica, primenljivi propisi i nadležnost sudova.

13. Odobrenje Komisije za hartije od vrednosti

Ovaj beli papir odobren je rešenjem Komisije za hartije od vrednosti Republike Srbije br. _____ od dana _____. Beli papir se ne može objaviti niti ponuditi javnosti bez prethodnog odobrenja Komisije.

14. Objavljivanje i izmene belog papira

Beli papir i sve njegove izmene biće javno objavljeni na zvaničnoj internet stranici izdavaoca i sajtu Komisije za hartije od vrednosti. Izmene belog papira odmah se objavljuju na istim mestima.

15. Odgovornost izdavaoca i lica koja su sačinila beli papir

Izdavalac, kao i lica koja su učestvovala u izradi belog papira, solidarno odgovaraju investitorima za štetu nastalu zbog netačnih, neistinitih ili nepotpunih podataka sadržanih u belom papiru.

16. Opoziv inicijalne ponude

Izdavalac zadržava pravo da opozove inicijalnu ponudu tokena pre njenog isteka. U slučaju opoziva, svi uplaćeni iznosi vraćaju se investitorima u roku od ____ dana, bez ikakvih troškova za investitore.

17. Čuvanje dokumentacije i dostupnost podataka

Izdavalac je dužan da čuva celokupnu dokumentaciju u vezi sa inicijalnom ponudom digitalne imovine najmanje 10 godina. Na zahtev investitora, izdavalac mora omogućiti uvid u dokumentaciju i pružiti sve relevantne informacije.

Iznošenje investicionog tokena na evropsko tržište (EU) – regulatorni i operativni plan

Ako bi želeli token napravljen za srpsko tržište da proširimo na tržište Evropske unije moramo se pridržavati zahtevima po **MiCA** uredbi, potencijalno primeniti **MiFID II/Prospectus** režim ako je token finansijski instrument, kao i obaveza kod pružanja usluga (CASP), AML/„travel rule“, pasportinga i tehničko-operativnim implikacijama.

MiCA – Regulation (EU) 2023/1114: jedinstvena pravila za kripto-imovinu koja **nije** već obuhvaćena finansijskim propisima EU. U potpunosti je operativna (u dve faze: od **30.06.2024.** za ART/EMT, i od **30.12.2024.** za ostale kripto-imovine i **CASP** autorizacije). **MiFID II / Prospekt:** ako kripto-imovina po svojim pravima funkcioniše kao **prenosivi hartijski papir** (npr. učešće u dobiti), ona **izlazi iz MiCA** i potpada pod postojeći režim za finansijske instrumente (MiFID II, Prospekt). ESMA je 2024/2025. objavila smernice kako odrediti kada kripto-imovina jeste finansijski instrument. **TFR („Travel rule“) – Regulation (EU) 2023/1113:** od **30.12.2024.** CASP-ovi moraju slati podatke o pošiljaocu/korisniku uz transfere kripto-imovine (ekvivalent pravilu o prenosu sredstava). **DLT Pilot Regime – (EU) 2022/858:** sandbox za trgovanje/naselja tokenizovanih finansijskih instrumenata; u 2025. u fazi preispitivanja sa opeijom produženja ili transformacije u trajni režim. **Passporting** je mehanizam jedinstvenog tržišta EU koji omogućava firmi **autorizovanoj u jednoj državi članici da preko slobode pružanja usluga ili osnivanja filijale** zakonito posluje u **svim ostalim državama članicama**, bez ponovnog licenciranja u svakoj od njih.

Kod našeg primera **LWT_1** daje pravo na **podelu profita** (50/50) nakon roka, što je tipično **investiciono pravo**. Po kriterijumima ESMA, takav token **vrlo verovatno** ispunjava definiciju **prenosivog hartijskog papira** (udzionički/dužnički karakter) i time postaje **finansijski instrument, nije** u MiCA, već u **MiFID II/Prospekt** režimu. Posledice su: prospekt (ili izuzeci), ovlašćeni posrednici, trgovačka infrastruktura (uklj. DLT Pilot ako je na DLT-u). Ako bi se token redizajnirao da **ne daje investiciona/dužničko-kapitalna prava** (npr. utility), tada bi pao pod MiCA (Titel II „other crypto-assets“), sa obavezom **crypto-asset white paper-a (CAWP)** i marketinškim pravilima.

Iz gore navedenog vidimo da imamo 2 regulatorne putanje za ulazak u EU. Security token“ putanja (verovatna za LWT_1) – MiFID II/Prospekt i „MiCA putanja“ (ako se token redizajnira u „other crypto-asset“).

Kod Security token“ putanje treba potvrditi da je LWT_1 prenosivi hartijski papir (legalna analiza po MiFID II + ESMA smernice), pripremiti i dobiti odobrenje **Prospekta** prema Uredbi 2017/1129 (ili primena izuzetaka za privatne ponude), uspostaviti saradnju sa ovlašćenim investicionim firmama/MTF,

pripremiti distribuciju i marketing po MiFID pravilima (fair, clear, not misleading) i u slučaju “on-chain settlement” pune obaveze za posrednike i pružaoce usluga kripto-imovine.

Kod „MiCA putanje” putanja prati izradu belog papira (CA White Paper), **obaveštavanje** nadležnog tela i **objava** pre ponude javnosti ili prijema na trgovanje (odgovornost za tačnost je na izdavaocu), **CASP licenca** (ako vi ili partner pružate usluge: prijem/transmisija naloga, skrbništvo, razmena, savetovanje itd.) što nakon odobrenja omogućava **pasporting** u celoj EU, pripremiti distribuciju i marketing po MiFID pravilima (fair, clear, not misleading) i primena pravila o „travel rule“ za CASP-ove.

Što se tiče našeg slučaja **MiCA ne predviđa** režim pružanja usluga iz trećih zemalja ka EU (bez prisustva) pa je praksa osnovati **EU pravno lice/filijalu** i tražiti dozvolu (**CASP**) u odabranoj državi članici (uz restriktivno i usko tumačenje “reverse solicitation”). Dok za **MiFID putanju** (security token) saradnja sa EU ovlašćenim posrednikom i relevantnim tržištem je neophodna (klasičnim ili DLT Pilot infrastrukturom).

Reference

1. Zakon o digitalnoj imovini - https://nbs.rs/export/sites/NBS_site/documents/propisi/zakoni/digitalna_imovina.pdf
2. Narodna banka Srbije – IPS NBS: pregled sistema za instant plaćanja (24/7/365) i osnovne karakteristike <https://www.nbs.rs/sr/ciljevi-i-funkcije/platni-sistem/nbs-operator/ips-nbs/>
3. NBS – IPS QR kod: standardizacija i upotreba za plaćanja. <https://ips.nbs.rs/en/ips-mesta-i-nacini-placanja/placanje-racuna-putem-nbs-ips-qr-koda>
4. Finspot Faktoring Token – FIN Beli pipir <https://finspot.com/wp-content/uploads/2022/06/Finspot-Beli-Papir.pdf>
5. Finspot Faktoring Token – FIN2 Beli pipir <https://finspot.com/wp-content/uploads/2023/01/Finspot-FIN-2-Beli-Papir.pdf>
6. Finspot Faktoring Token – FIN3 Beli pipir <https://finspot.com/wp-content/uploads/2024/03/Finspot-FIN-3-Beli-Papir.pdf>
7. The Walnut Enterprise – TWE_L2 Beli papir (2025) <https://thewalnutfund.com/documents/TWE-Beli-Papir-16.05.2024.pdf>
8. Virtus vinski token – Beli papir (Solana/SPL) https://klub.vinarijavirtus.rs/assets/Whitepaper_new.pdf
9. ERC-20: Token Standard (EIP-20) <https://eips.ethereum.org/EIPS/eip-20>
10. OpenZeppelin Contracts – ERC-20 vodič i API (v5.x) <https://docs.openzeppelin.com/contracts/5.x/erc20>
11. ERC-4626: Tokenized Vaults (EIP-4626) <https://eips.ethereum.org/EIPS/eip-4626>
12. OpenZeppelin Contracts – ERC-4626 referenca (v5.x) <https://docs.openzeppelin.com/contracts/5.x/erc4626>
13. Metaplex (Solana) – Token Metadata: pregled i Token Standard <https://developers.metaplex.com/token-metadata>

14. Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-assets (MiCA), Official Journal <https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng>
15. Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets (TFR – “travel rule”), Official Journal <https://eur-lex.europa.eu/eli/reg/2023/1113/oj/eng>
16. Regulation (EU) 2017/1129 (Prospectus Regulation), Official Journal <https://eur-lex.europa.eu/eli/reg/2017/1129/oj/eng>
17. Directive 2014/65/EU (MiFID II), Official Journal <https://eur-lex.europa.eu/eli/dir/2014/65/oj/eng>
18. Regulation (EU) 2022/858 (DLT Pilot Regime), Official Journal <https://eur-lex.europa.eu/eli/reg/2022/858/oj/eng>
19. ESMA Guidelines on reverse solicitation under MiCA (ESMA35-1872330276-2030) <https://www.esma.europa.eu/document/guidelines-reverse-solicitation-under-mica>