



UNIVERZITET U BEOGRADU  
EKONOMSKI FAKULTET



UNIVERZITET U BEOGRADU  
Ekonomski fakultet

**MASTER TEZA**

# **DIGITALNE TEHNOLOGIJE U BANKARSTVU**

student:

Stefan Janković 2667/2022

mentor:

dr Đorđe Stakić

BEOGRAD  
MAJ 2025.

## SAŽETAK

Ovaj master rad analizira uticaj digitalnih tehnologija na efikasnost, bezbednost i korisničko iskustvo u bankarskom sektoru Srbije. Digitalizacija omogućava brže transakcije, smanjuje operativne troškove i poboljšava dostupnost bankarskih usluga, ali istovremeno donosi izazove vezane za sajber bezbednost, regulatorne zahteve i poverenje korisnika. Cilj istraživanja je identifikacija ključnih faktora digitalne transformacije i predlaganje mera za optimizaciju bankarskih usluga. Istraživanje je sprovedeno korišćenjem kvantitativne metodologije, kroz strukturisanu anketu sa učesnicima. Anketiranje je izvršeno uz pomoć ankete koja je kreirana na Google forms aplikaciji, na osnovu koje su analizirani podaci o rasprostranjenosti primene mobilnog bankarstva, korisnička iskustva i rizici. Rezultati ukazuju na to da mobilno bankarstvo pozitivno utiče na efikasnost bankarskih usluga, a i samu konkurentnost banaka, dok istovremeno zahteva dodatne mere zaštite i regulatornog usklađivanja. Preporučuje se unapređenje sigurnosne infrastrukture, jačanje transparentnosti i uvođenje inovativnih digitalnih rešenja koja povećavaju poverenje korisnika.

**Ključne reči:** digitalne tehnologije, bankarstvo, efikasnost, bezbednost, digitalizacija.

## **ABSTRACT**

This master's thesis analyzes the impact of digital technologies on efficiency, security and user experience in the Serbian banking sector. Digitalization enables faster transactions, reduces operating costs and improves the availability of banking services, but at the same time brings challenges related to cybersecurity, regulatory requirements and user trust. The aim of the research is to identify key factors of digital transformation and propose measures for optimizing banking services. The research was conducted using quantitative methodology, through a structured survey with participants. The survey was conducted using a survey created on Google Forms application, based on which data on the prevalence of mobile banking, user experiences and risks were analyzed. The results indicate that mobile banking has a positive impact on the efficiency of banking services and the competitiveness of banks, while at the same time requiring additional protection measures and regulatory compliance. It is recommended to improve the security infrastructure, strengthen transparency and introduce innovative digital solutions that increase user trust.

Keywords: digital technologies, banking, efficiency, security, digitization.



UNIVERZITET U BEOGRADU  
Ekonomski fakultet

### Izjava o korišćenju licnih podataka

Dozvoljavam da se objave moji licni podaci vezani za dobijanje akademskog naziva master ekonomiste, kao što su ime i prezime, godina i mesto rođenja i datum odbrane rada.

Ovi licni podaci mogu se objaviti na mrežnim stranicama digitalne biblioteke, u elektronskom katalogu i u publikacijama Univerziteta u Beogradu – Ekonomskog fakulteta.

Ovlašćujem biblioteku Univerziteta u Beogradu – Ekonomskog fakulteta da u svoj digitalni repozitorijum unese moj završni (master) rad pod naslovom:

Digitalne tehnologije u bankarstvu

koji je moje autorsko delo.

Završni (master) rad sa svim prilogima predao/la sam u elektronskom formatu pogodnom za trajno arhiviranje.

Moj završni (master) rad, pohranjen u Digitalnom repozitorijumu Univerziteta u Beogradu – Ekonomskog fakulteta i dostupan u otvorenom pristupu, mogu da koriste svi koji poštuju odredbe sadržane u CC BY licenci Kreativne zajednice (Creative Commons), a kojom je dozvoljeno umnožavanje, distribucija i javno saopštavanje dela, i prerade, uz adekvatno navođenje imena autora, čak i u komercijalne svrhe.

U Beogradu, 14.02.2025.

Potpis autora

M. Stanković



### Izjava o akademskoj ceditosti

Student/kinja: Stefan Janković

Broj indeksa: 2667/2012

Autor/ka master rada pod nazivom:

Digitalne tehnologije u bankarstvu

Potpisivanjem izjavljujem:

- da je rad isključivo rezultat mog sopstvenog istraživačkog rada;
- da sam rad i mišljenja drugih autora koje sam koristio/la u ovom radu naznačio/la ili citirao/la u skladu sa Uputstvom;
- da su svi radovi i mišljenja drugih autora navedeni u spisku literature/referenci koji su sastavni deo ovog rada i pisani u skladu sa Uputstvom; o da sam dobio/la sve dozvole za korišćenje autorskog dela koji se u potpunosti/celosti unose u predati rad i da sam to jasno naveo/la;
- da sam svestan/na da je plagijat korišćenje tuđih radova u bilo kom obliku (kao citata, parafraza, slika, tabela, dijagrama, dizajna, planova, fotografija, filma, muzike, formula, veb sajtova, kompjuterskih programa i sl.) bez navođenja autora ili predavljanje tuđih autorskih dela kao mojih, kažnjivo po zakonu (Zakon o autorskom i srodnim pravima, Službeni glasnik Republike Srbije, br. 104/2009, 99/2011, 119/2012), kao i drugih zakona i odgovarajućih akata Univerziteta u Beogradu;
- da sam da sam svestan/na da plagijat uključuje i predavljanje, upotrebu i distribuiranje rada predavaca ili drugih studenata kao sopstvenih;
- da sam svestan/na posledica koje kod dokazanog plagijata mogu prouzrokovati na predati master rad i moj status;
- da je elektronska verzija master rada identična štampanom primerku i pristajem na njegovo objavljivanje pod uslovima propisanim aktima Univerziteta.

Beograd, 14.02.2015.

Potpis [Signature]

|                                                                              |    |
|------------------------------------------------------------------------------|----|
| SAŽETAK .....                                                                | 2  |
| ABSTRACT.....                                                                | 3  |
| UVOD .....                                                                   | 8  |
| 1 DIGITALNE TEHNOLOGIJE U BANKARSTVU.....                                    | 9  |
| 1.1 Razvoj digitalnog bankarstva .....                                       | 9  |
| 1.2 Koncepti digitalnih usluga u bankarstvu .....                            | 11 |
| 1.3 Mobilno i internet bankarstvo .....                                      | 13 |
| 1.4 Digitalna plaćanja i transakcije .....                                   | 15 |
| 1.4.1 Digitalni novac i kriptovalute .....                                   | 16 |
| 1.4.2 Onlajn plaćanja .....                                                  | 18 |
| 1.4.3 Plaćanja putem kartica i QR kodova.....                                | 20 |
| 1.4.4 Digitalni novčanici.....                                               | 24 |
| 2 IZAZOVI I RIZICI DIGITALNIH TEHNOLOGIJA U BANKARSTVU .....                 | 27 |
| 2.1 Bezbednost digitalnog novca i kriptovaluta .....                         | 27 |
| 2.1.1 Arhitektura bezbednosti .....                                          | 27 |
| 2.1.2 Modeli bezbednosti: ključne komponente i primena u kriptovalutama..... | 29 |
| 2.1.3 Sigurni metodi prenosa podataka.....                                   | 31 |
| 2.2 Regulatorni izazovi u primeni digitalnih tehnologija u bankarstvu .....  | 33 |
| 2.2.1 Digitalno bankarstvo danas.....                                        | 33 |
| 2.2.2 Licenciranje digitalnih banaka i regulatorni pristupi .....            | 34 |
| 2.2.3 Izazovi u primeni regulative .....                                     | 36 |
| 2.2.4 Specifični izazovi u digitalizaciji bankarstva .....                   | 38 |
| 2.2.5 Primeri regulatornih pristupa .....                                    | 41 |
| 2.3 Izazovi u onlajn plaćanjima i elektronskom načinu plaćanja.....          | 46 |
| 2.3.1 Onlajn plaćanja i bezbednosni izazovi u digitalnim transakcijama ..... | 47 |

|       |                                                                         |    |
|-------|-------------------------------------------------------------------------|----|
| 2.3.2 | Prepoznavanje izazova kod elektronskih plaćanja.....                    | 48 |
| 2.4   | Sprečavanje prevara i zaštita podataka u digitalnim transakcijama ..... | 49 |
| 2.4.1 | Uobičajeni primeri digitalnih prevara .....                             | 50 |
| 2.4.2 | Otkrivanje i sprečavanje bankarskih prevara .....                       | 50 |
| 2.4.3 | Strategije za borbu protiv prevara u bankarstvu .....                   | 51 |
| 2.4.4 | Napadi socijalnog inženjeringa i mere zaštite .....                     | 52 |
| 3     | UTICAJ DIGITALNIH TEHNOLOGIJA NA BANKARSKI SEKTOR U SRBIJI .....        | 54 |
| 3.1   | Analiza trenutnog stanja digitalizacije .....                           | 54 |
| 3.2   | Uticaj digitalnih tehnologija na efikasnost poslovanja .....            | 56 |
| 3.3   | Zadovoljstvo klijenata i korisničko iskustvo.....                       | 59 |
| 3.4   | Unapređenje sigurnosti i konkurentnosti.....                            | 63 |
| 3.5   | Primeri iz prakse i empirijsko istraživanje.....                        | 64 |
| 3.5.1 | Primeri iz prakse .....                                                 | 65 |
| 3.5.2 | Empirijsko istraživanje .....                                           | 67 |
| 4     | PREPORUKE ZA UNAPREĐENJE DIGITALNIH USLUGA U BANKARSTVU SRBIJE          |    |
|       | 73                                                                      |    |
| 4.1   | Strategije za optimizaciju digitalnih procesa .....                     | 73 |
| 4.2   | Poboljšanje korisničkog iskustva .....                                  | 75 |
| 4.3   | Povećanje bezbednosti digitalnih transakcija.....                       | 76 |
| 4.4   | Predlozi za dalji razvoj digitalnih usluga .....                        | 78 |
|       | ZAKLJUČAK.....                                                          | 80 |
|       | LITERATURA .....                                                        | 82 |
|       | SPISAK KORIŠĆENIH SKRAĆENICA .....                                      | 86 |
|       | PRILOG: UPITNIK.....                                                    | 88 |

## UVOD

Digitalna transformacija predstavlja jednu od najvažnijih promena u savremenom poslovanju, a njen uticaj je posebno izražen u bankarskom sektoru. Uvođenje digitalnih tehnologija, poput mobilnog bankarstva, veštačke inteligencije i blokčejna (engl. blockchain), značajno je unapredilo efikasnost, sigurnost i dostupnost finansijskih usluga. Ova tema je od suštinske važnosti jer digitalizacija redefiniše način na koji banke funkcionišu, povećavajući brzinu transakcija, dok istovremeno postavlja nove izazove u pogledu bezbednosti i regulative.

Razlozi odabira teme proizlaze iz sve veće potrebe za razumevanjem prednosti i prepreka digitalizacije u bankarstvu, posebno u Srbiji, gde sektor finansija prolazi kroz ubrzane procese modernizacije. Digitalne platforme pružaju korisnicima lakši pristup uslugama, smanjuju troškove i povećavaju konkurentnost banaka, ali istovremeno otvaraju pitanja o sajber bezbednosti i pravnoj usklađenosti.

Naime, digitalni novac i tehnologije menjaju globalnu ekonomiju, redefinišući ulogu tradicionalnog bankarstva. Upravo to potvrđuje relevantnost istraživanja uticaja novih tehnologija na efikasnost i sigurnost bankarskih procesa, čime se obezbeđuje osnov za bolje razumevanje njihove primene u lokalnom kontekstu.

Cilj ovog rada je istražiti kako digitalne tehnologije utiču na bankarski sektor u Srbiji, sa posebnim naglaskom na efikasnost, bezbednost i zadovoljstvo korisnika. Fokus je na analizi trenutnih trendova i izazova, kao i na davanju preporuka za unapređenje digitalnih usluga, čime se doprinosi daljoj modernizaciji i konkurentnosti bankarskog sektora u savremenom digitalnom okruženju.

Struktura master rada obuhvata uvod, četiri glavna poglavlja i zaključak. Uvod predstavlja aktuelnost teme, ciljeve i metodologiju. Prvo poglavlje razmatra razvoj digitalnih tehnologija u bankarstvu, uključujući mobilno i internet bankarstvo, digitalni novac i onlajn plaćanja. Drugo poglavlje istražuje izazove i rizike, poput bezbednosti i regulatornih pitanja. Treće poglavlje analizira uticaj digitalizacije na bankarski sektor u Srbiji, fokusirajući se na efikasnost, sigurnost i korisničko iskustvo. Četvrto poglavlje sadrži preporuke za unapređenje digitalnih usluga u Srbiji. Rad se završava zaključkom i spiskom literature.

# 1 DIGITALNE TEHNOLOGIJE U BANKARSTVU

U razvoju digitalnog bankarstva značajno je pomenuti njegove ključne koncepte koji su temelj savremene transformacije finansijskih usluga. Tehnološki napredak omogućio je da tradicionalni modeli poslovanja evoluiraju ka bržim, dostupnijim i personalizovanim rešenjima. Mobilno i internet bankarstvo postali su svakodnevni alati korisnika, dok digitalna plaćanja, uključujući transakcije putem kartica, QR kodova i onlajn servisa, redefinišu način obavljanja finansijskih aktivnosti. Paralelno s tim, rast primene kriptovaluta i digitalnih novčanika dodatno su proširili spektar digitalnih mogućnosti, postavljajući nove standarde efikasnosti, sigurnosti i kontrole nad ličnim finansijama.

## 1.1 Razvoj digitalnog bankarstva

Digitalno bankarstvo predstavlja suštinsku prekretnicu u savremenom finansijskom sistemu, preobražavajući način na koji pojedinci i preduzeća upravljaju svojim finansijama. Kroz neprekidnu evoluciju tehnoloških rešenja, bankarski sektor je prešao put od tradicionalnih šaltera do sofisticiranih digitalnih platformi koje omogućavaju obavljanje transakcija u realnom vremenu, bez obzira na geografsku lokaciju. Ovaj proces, koji je inicijalno započeo automatizacijom osnovnih bankarskih operacija, danas je prerastao u sveobuhvatnu transformaciju poslovnih modela i korisničkih iskustava (OECD, 2020).

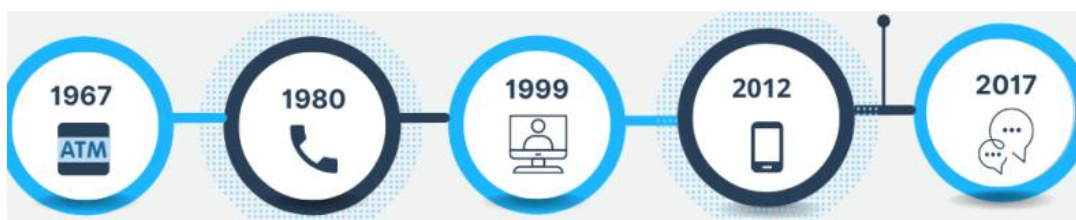
Povezivanjem korisnika s bankama kroz digitalne kanale, stvorena je nova dimenzija interakcije zasnovana na personalizaciji i brzini. Suštinu prilagođavanja bankarskog sektora savremenim zahtevima i digitalnim trendovima oslikava krilatica da je promena zakon života, a oni koji gledaju samo u prošlost ili u sadašnjost propustiće budućnost (Osterwalder, Pigneur, & Tucci, 2005).

Prvi koraci digitalnog bankarstva datiraju još iz šezdesetih godina prošlog veka, kada su banke počele koristiti računare za automatizaciju funkcija poput obrade čekova i upravljanja računima. Razvoj bankomata, koji je omogućio podizanje novca bez odlaska na šalter, predstavljao je ključnu inovaciju tog doba. Tokom osamdesetih godina, uvođenje onlajn bankarstva putem *dial-up* konekcija omogućilo je klijentima pristup informacijama o svojim računima (Revathi, 2019).

Devedesete godine donele su masovniju upotrebu interneta, što je otvorilo prostor za razvoj portala za onlajn bankarstvo. Banke su počele nuditi mogućnosti plaćanja računa, transfera sredstava i

provere stanja sa kućnih računara. Primer je Wells Fargo, koji je 1996. godine omogućio svojim klijentima pristup onlajn servisima, čime je digitalno bankarstvo dodatno unapređeno.

Razvojem pametnih telefona i aplikacija, korisnici su dobili mogućnost upravljanja računima u pokretu, vršenja transakcija i plaćanja računa s lakoćom. Ovaj trend je dodatno ojačan pojavom USAA Federal Savings Bank, koja je 2007. godine prva uvela mobilnu aplikaciju za bankarstvo.



Slika 1. Evolucija digitalnog bankarstva (OECD, 2020).

Slika 1 prikazuje hronološku evoluciju digitalizovanog bankarstva od 1967. do 2017. godine, ističući ključne inovacije koje su transformisale finansijski sektor. Proces započinje uvođenjem bankomata (ATM) 1967. godine, koji je omogućio korisnicima pristup gotovini bez potrebe za fizičkim odlaskom u banku. Godine 1980. dolazi do razvoja telefonskog bankarstva, čime su klijenti mogli izvršavati transakcije i proveravati stanje računa putem telefona. Kasnije, 1999. godine, pojavljuje se internet bankarstvo (engl. Online Banking), pružajući korisnicima mogućnost obavljanja finansijskih usluga putem interneta, čime je bankarstvo postalo dostupnije i efikasnije. U 2012. godini dolazi do razvoja mobilnog bankarstva (engl. Mobile Banking), koje je omogućilo korisnicima obavljanje transakcija, plaćanja i pristup finansijama putem pametnih telefona. Prekretnica dolazi 2017. godine s pojavom konverzijskog bankarstva (engl. Conversational Banking), koje koristi čet-botove (engl. chatbot) i AI tehnologije za personalizovanu komunikaciju i automatizovane usluge, uz istovremeno uvođenje koncepta otvorenog bankarstva (engl. Open Banking), omogućavajući povezivanje sa trećim stranama radi proširivanja finansijskih usluga. AI tehnologije smanjuju rizik od prevara za 35%, a banke koje koriste AI asistente beleže 20%, veću stopu korisničkog zadovoljstva u odnosu na tradicionalne metode pružanja usluga (OECD, 2020). Ovaj dijagram ističe kontinuiranu digitalnu transformaciju bankarstva, prilagođavajući se potrebama modernih korisnika i tehnološkim inovacijama.

Uvođenje mobilnog bankarstva kao jednog od ključnih segmenata digitalizacije omogućilo je brzu i laku realizaciju finansijskih transakcija, dok su napredne funkcionalnosti, poput biometrijske

autentifikacije i tokenizacije, podigle nivo sigurnosti na novi nivo. Paralelno s tim, razvoj internet bankarstva obuhvatio je širok spektar funkcija, od uvida u stanje računa do kompleksnih investicionih operacija, pružajući korisnicima jednostavnost i efikasnost na svakom koraku (Pavithra & Geetha, 2021).

Jedan od ključnih pokretača digitalne transformacije bio je odgovor na rastuće zahteve korisnika za većom fleksibilnošću i praktičnošću. Pandemija COVID-19 dodatno je ubrzala ovaj proces, ističući značaj digitalnih rešenja za kontinuitet poslovanja i održavanje finansijske stabilnosti (PWC, 2016).

Današnji razvoj digitalnog bankarstva uključuje napredne tehnologije poput blokčejna, koji omogućava sigurnije i efikasnije transakcije. Integracija veštačke inteligencije doprinosi automatizaciji korisničke podrške putem čet-botova i virtuelnih asistenata, dok biometrijske metode autentifikacije povećavaju sigurnost.

Transformacija se ne završava, već se neprekidno prilagođava novim tehnološkim dostignućima i očekivanjima korisnika, oblikujući budućnost finansijskih usluga u skladu sa savremenim izazovima i mogućnostima.

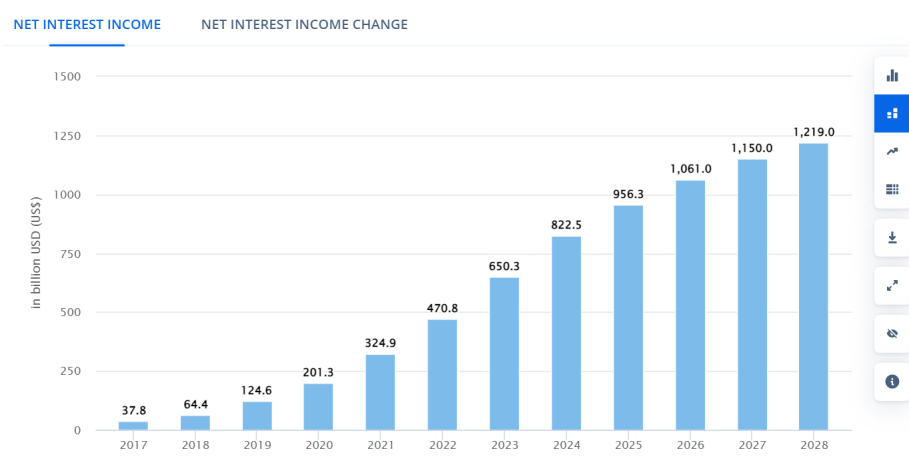
U budućnosti digitalno bankarstvo će se oslanjati na IoT tehnologije, koje će omogućiti praćenje finansijskih navika u realnom vremenu i pružanje personalizovanih saveta. Pored toga, blokčejn i decentralizovane finansije (DeFi) postavljaju temelje za još veću sigurnost i transparentnost transakcija, smanjujući ulogu posrednika. Većina banaka u Srbiji koristi višeslojnu zaštitu podataka, uključujući algoritme enkripcije i multifaktorsku autentifikaciju, što je u skladu sa preporukama Evropske centralne banke (Stankić, Lukić, & Popović, 2023). Ove mere su neophodne za smanjenje rizika od sajber napada i povećanje poverenja korisnika u digitalne kanale. Iako DeFi nudi inovativne mogućnosti, digitalno bankarstvo ostaje dominantno zbog svoje stabilnosti i šire primene.

## **1.2 Koncepti digitalnih usluga u bankarstvu**

Digitalno bankarstvo predstavlja modernizovanu verziju tradicionalnog bankarstva, koja koristi savremene digitalne tehnologije za pružanje finansijskih usluga putem interneta i mobilnih aplikacija. Njegov osnovni cilj je omogućavanje korisnicima pristupa bankarskim uslugama bilo

kada i bilo gde, bez potrebe za fizičkim prisustvom u poslovnica (Osterwalder et al., 2005). Ovaj koncept obuhvata širok spektar funkcija, uključujući upravljanje računima, elektronska plaćanja, mobilno bankarstvo i aplikacije zasnovane na veštačkoj inteligenciji, što omogućava optimizaciju korisničkog iskustva.

Prikazana slika 2. ilustruje rast neto prihoda od kamata (engl. Net Interest Income) u milijardama američkih dolara (USD) od 2017. do 2028. godine, sa jasno izraženim trendom stalnog povećanja. Početna vrednost u 2017. iznosila je 37,8 milijardi USD, dok se predviđa da će do 2028. godine dostići 1.219,0 milijardi USD. Ovaj rast sugerise kontinuirano širenje i povećanje profitabilnosti u bankarskom sektoru, uz značajan porast nakon 2020. godine. Primetan je ubrzan rast od 2021. do 2025. godine, nakon čega tempo rasta postaje postepeniji. Za banke, digitalizacija dovodi do smanjenja operativnih troškova i povećanja profitabilnosti kroz automatizaciju procesa, dok širenje digitalnog bankarstva doprinosi rastućoj potražnji za kreditima, kamatnim prihodima i efikasnijem prikupljanju prihoda putem novih tehnologija i optimizacije poslovanja.



Slika 2. Neto prihod digitalnog bankarstva 2017-2028 (<https://www.statista.com/> )

Primena digitalnog bankarstva donosi višestruke koristi, uključujući efikasnost, dostupnost i uštedu vremena, omogućavajući korisnicima da brzo, sigurno i u bilo kojem trenutku obavljaju transakcije, plaćanja i provere stanja računa, čime se povećava fleksibilnost i bolja kontrola finansija (Pavithra & Geetha, 2021). Osim toga, integracija naprednih analitičkih alata i personalizovanih usluga, zasnovanih na veštačkoj inteligenciji, omogućava korisnicima preciznije upravljanje budžetom i donošenje finansijskih odluka (PWC, 2016). Dalje, digitalne platforme

pružaju naprednu zaštitu podataka putem enkripcije, višefaktorske autentifikacije i stalnog nadzora transakcija, čime se jača poverenje korisnika.

Digitalno bankarstvo omogućava korisnicima pristup bankovnim uslugama putem različitih kanala, uključujući internet bankarstvo na računarima ili laptopima za obavljanje plaćanja i upravljanje računima, kao i mobilno bankarstvo putem pametnih telefona i tableta, s naglaskom na brzinu i praktičnost transakcija. Idealan je za korisnike koji preferiraju rad sa većim ekranima i dodatnim funkcionalnostima (Revathi, 2019). Digitalne platforme, uključujući mobilno bankarstvo, omogućavaju brze transakcije i mobilna plaćanja, uz naprednu zaštitu podataka kroz enkripciju, višefaktorsku autentifikaciju i stalni nadzor transakcija, čime se jača poverenje korisnika i obezbeđuje sigurnost u svim digitalnim interakcijama (Sayed & Sayed, 2020). Neobanke (engl. Challenger banke) su potpuno digitalne banke koje funkcionišu bez fizičkih poslovnica. Nude inovativna rešenja poput direktnog ulaganja u kriptovalute i integrisanih aplikacija za finansijsko upravljanje (Schmidt-Jessa, 2023). *Fintech* platforme su specijalizovane aplikacije koje pružaju pojedinačne finansijske usluge poput upravljanja budžetom, investicija i međunarodnih plaćanja<sup>1</sup>. Njihova fleksibilnost omogućava brzo prilagođavanje tržišnim potrebama (Shahid, Islam, Malik, & Hasan, 2022). Najzad, elektronski platni sistemi su fokusirani na omogućavanje brzih i sigurnih transakcija, uključujući mobilna plaćanja, elektronske novčanike i beskontaktnu tehnologiju (Stankić et al., 2023).

### **1.3 Mobilno i internet bankarstvo**

Mobilno i internet bankarstvo predstavljaju ključne segmente savremenog digitalnog bankarstva, pružajući korisnicima fleksibilnost i efikasnost u upravljanju finansijama. Iako oba oblika omogućavaju daljinsko obavljanje transakcija i upravljanje računima, postoje značajne razlike u njihovim funkcionalnostima, pristupačnosti i sigurnosnim mehanizmima koje ih čine pogodnim za različite korisničke potrebe.

Mobilno bankarstvo se oslanja na upotrebu pametnih telefona i tableta, omogućavajući korisnicima pristup finansijskim uslugama putem mobilnih aplikacija ili prilagođenih veb

---

<sup>1</sup> FinTech kompanije sve više ugrožavaju tradicionalne banke svojim inovacijama, primoravajući ih na ubrzanu digitalizaciju. Na primer, Revolut i N26 su osvojili milione korisnika zahvaljujući jednostavnim i pristupačnim digitalnim platformama.

interfejsa. Njegova glavna prednost leži u praktičnosti, jer korisnici mogu obavljati transakcije u pokretu, bilo kada i bilo gde, pod uslovom da imaju pristup internetu (Khuong, Phuong, Liem, Thuy, & Son, 2022). Mobilno bankarstvo omogućava brze i jednostavne transakcije, kao što su plaćanja, prenos sredstava i upravljanje kreditima, dok internet bankarstvo nudi detaljniji uvid u finansije i pogodnije je za složenije transakcije, kao što su međunarodni transferi ili upravljanje višestrukim računima (Murinde, Rizopoulos, & Zachariadis, 2022; Mandic, Delibasic, Knezevic, & Benkovic, 2014).

Jedna od ključnih razlika između ova dva modela je pristupačnost (videti Tabelu 1). Mobilno bankarstvo je popularno među mlađim korisnicima i onima koji često putuju, dok internet bankarstvo preferiraju poslovni korisnici i oni koji obavljaju složenije finansijske operacije (Milošević, Dobrota, & Barjaktarović Rakočević, 2018).

Sigurnost je ključna u oba oblika bankarstva, pri čemu mobilno bankarstvo koristi biometrijsku autentifikaciju (otisci prstiju, prepoznavanje lica), dok internet bankarstvo primenjuje višeslojne zaštite poput SSL (engl. Secure Sockets Layer) enkripcije i dvofaktorske autentifikacije (OECD, 2020). Ova kombinacija mera osigurava visok nivo zaštite podataka i transakcija na obe platforme.

Prema podacima iz Tabele 1, mobilno i internet bankarstvo imaju komplementarne uloge u modernom finansijskom ekosistemu. Dok mobilno bankarstvo pruža neuporedivu fleksibilnost i pristupačnost, internet bankarstvo ostaje ključni alat za detaljniju analizu i upravljanje složenijim finansijskim operacijama. Kombinacija ovih tehnologija omogućava korisnicima da prilagode svoje bankarske potrebe prema individualnim navikama i preferencijama, čime se dodatno unapređuje korisničko iskustvo i jača poverenje u digitalne finansijske servise.

Tabela 1. Poređenje mobilnog i internet bankarstva (OECD, 2020).

| Osnova za poređenje     | Mobilno bankarstvo                                                                                                              | Internet bankarstvo                                                                                                                 |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| <b>Značenje</b>         | Mobilno bankarstvo podrazumeva internet uslugu banaka koja omogućava klijentima izvršavanje transakcija putem mobilnih uređaja. | Internet bankarstvo predstavlja uslugu koja korisnicima omogućava obavljanje finansijskih transakcija elektronski, putem interneta. |
| <b>Uređaji</b>          | Mobilni telefoni ili tableti                                                                                                    | Računari ili laptopi                                                                                                                |
| <b>Korišćenje</b>       | SMS, mobilne aplikacije ili optimizovane veb stranice                                                                           | Veb stranica banke                                                                                                                  |
| <b>Prenos sredstava</b> | Preko NEFT, RTGS ili UPI sistema                                                                                                | Preko NEFT, RTGS, IMPS i drugih sistema                                                                                             |
| <b>Funkcije</b>         | Ograničene funkcije – provera stanja, transfer novca, plaćanje računa                                                           | Šire funkcionalnosti – otvaranje računa, investicije, ažuriranje podataka, prijava za kredite i kartice                             |
| <b>Bezbednost</b>       | Biometrijska autentifikacija (otisci prstiju, prepoznavanje lica) i šifre za prijavu                                            | SSL enkripcija, dvofaktorska autentifikacija i sigurnosni tokeni                                                                    |
| <b>Pristupačnost</b>    | Visoka – dostupan bilo kada i bilo gde putem mobilnih mreža                                                                     | Ograničenija – zahteva računar i stabilnu internet konekciju                                                                        |
| <b>Praktičnost</b>      | Veća fleksibilnost i pogodnost za korisnike u pokretu                                                                           | Pogodnije za kompleksnije transakcije koje zahtevaju detaljan pregled i veće ekrane                                                 |
| <b>Notifikacije</b>     | Trenutna obaveštenja putem push poruka i SMS-a                                                                                  | Imejl obaveštenja i periodični izveštaji                                                                                            |
| <b>Ciljna grupa</b>     | Korisnici koji preferiraju brzo i jednostavno bankarstvo u pokretu                                                              | Korisnici koji više koriste statične uređaje za detaljne analize i kompleksne operacije                                             |

Analize pokazuju da digitalizacija bankarskog sektora doprinosi povećanju konkurentnosti i performansi banaka, omogućavajući smanjenje troškova poslovanja i povećanje zadovoljstva klijenata (Stefanovic, Barjaktarovic, & Bataev, 2021). Istovremeno, digitalna transformacija nosi određene izazove, uključujući potrebu za kontinuiranim unapređenjem sigurnosnih sistema i prilagođavanjem regulatornim okvirima (Milosevic, Dobrota, Dmitrovic, & Barjaktarovic Rakocovic, 2021).

## 1.4 Digitalna plaćanja i transakcije

Savremeni finansijski sistemi suočavaju se sa dubokim transformacijama usled razvoja digitalnog novca i kriptovaluta. Ove tehnologije redefinišu tradicionalne modele plaćanja, omogućavajući brže, sigurnije i efikasnije transakcije. Digitalizacija finansija je primer kako inovacije oblikuju ekonomske tokove i društvo.

### 1.4.1 Digitalni novac i kriptovalute

Digitalni novac je elektronski oblik sredstava koji omogućava obavljanje transakcija putem interneta, a centralizovan je i pod nadzorom finansijskih institucija, što garantuje njegovu stabilnost i sigurnost. Njegova ključna karakteristika je nematerijalnost – ne postoji u fizičkom obliku poput gotovine ili kovanica, već se skladišti u digitalnim novčanicima i bankarskim računima. Ovaj koncept obuhvata širok spektar valuta, uključujući elektronski novac (engl. e-money), centralnbankarske digitalne valute (engl. CBDC)<sup>2</sup> i kriptovalute. Primeri digitalnog novca uključuju PayPal, Venmo i WebMoney, koji omogućavaju plaćanja putem aplikacija i računara, pri čemu transakcije nadziru regulisane institucije. Njegova praktičnost omogućava jednostavan pristup finansijama i integraciju sa modernim tehnologijama. Digitalni novac oslanja se na poverenje u emitente, često banke ili druge institucije, koje garantuju njegovu stabilnost i sigurnost (Stankić, 2021).

Kriptovalute predstavljaju poseban oblik digitalnog novca koji se zasniva na kriptografiji i blokčejn tehnologiji. Njihova osnovna karakteristika je decentralizacija – transakcije se potvrđuju unutar mreže korisnika bez posredstva centralnih autoriteta. Prva kriptovaluta, *Bitcoin*, pojavila se 2008. godine kao odgovor na nezadovoljstvo tradicionalnim bankarskim sistemima. Danas, *Ethereum*, *Ripple*<sup>3</sup> i *Litecoin* nude dodatne funkcionalnosti poput pametnih ugovora<sup>4</sup>, koji automatizuju transakcije i smanjuju potrebu za posrednicima. Kriptovalute nude moć u rukama korisnika omogućavajući im direktno upravljanje sredstvima bez kontrole banaka (Vives, 2019).

Digitalni novac i kriptovalute predstavljaju dva različita oblika elektronskog plaćanja, a njihove razlike leže u načinu funkcionisanja, sigurnosti i pravnoj regulativi. Decentralizovane blokčejn mreže kriptovaluta omogućavaju veću autonomiju korisnicima i povećavaju transparentnost, jer su svi podaci javno zabeleženi na distribuiranim knjigama zapisa, čime se smanjuje mogućnost manipulacija. Dok digitalni novac omogućava povrat sredstava u slučaju greške, transakcije kriptovalutama su nepovratne, pružajući veću transparentnost, ali i veću odgovornost korisnicima.

---

<sup>2</sup> CBDC predstavlja digitalnu verziju fiat valute koju izdaju centralne banke. Ove valute kombinuju sigurnost tradicionalnog bankarskog sistema sa prednostima digitalnih tehnologija.

<sup>3</sup> Ripple (XRP) je digitalna valuta dizajnirana za brze i jeftine međunarodne transfere novca. Koristi konsenzus protokol, umesto tradicionalnih konsenzus algoritama poput PoW i PoS, što omogućava kraće vreme transakcije.

<sup>4</sup> Pametni ugovori (engl. smart contracts) su programski kodovi na blokčejnu koji automatski izvršavaju ugovorene uslove između strana bez potrebe za posrednicima

Digitalni novac je široko regulisan u većini zemalja, dok pravni status kriptovaluta zavisi od specifičnih pravnih okvira koji se još uvek razvijaju. Kako je primećeno, tehnologija nije ni dobra ni loša, ali njen uticaj zavisi od toga kako se koristi – upravo te razlike definišu ulogu ovih instrumenata u savremenom finansijskom sistemu.

Digitalni novac i kriptovalute donose brojne prednosti, uključujući brže transakcije, niže troškove obrade i pristup globalnim tržištima. Dok digitalni novac osigurava stabilnost i poverenje putem centralizovanih institucija, kriptovalute pružaju veću sigurnost, autonomiju i transparentnost zahvaljujući decentralizovanoj prirodi (Stankić, 2021; Vives, 2019). Kriptovalute se često koriste kao zaštita od inflacije, naročito u zemljama sa nestabilnim ekonomijama, pružajući alternativu tradicionalnim valutama i postajući privlačan izbor za investitore. Naredna tabela 2. pruža pregled ključnih podataka o rastu i uticaju kriptovaluta širom sveta, naglašavajući njihovu popularnost, prihvaćenost u poslovanju i izazove poput pranja novca.

Tabela 2. Statistika o kriptovalutama (Stefanovic et al., 2021).

| Statistika                       | Podaci                                                                                            |
|----------------------------------|---------------------------------------------------------------------------------------------------|
| <b>Globalni korisnici</b>        | Preko 450 miliona korisnika kriptovaluta u novembru 2023. godine.                                 |
| <b>Tržište bankomata (ATM)</b>   | Globalno tržište bankomata za kriptovalute vredeće 91,8 milijardi dolara do 2028. godine.         |
| <b>Bitcoin (<i>Bitcoin</i>)</b>  | Bitkoini su bili najpopularnije kriptovalute među hedž fondovima u 2023. godini.                  |
| <b>Vlasnici <i>Etherum</i></b>   | Broj vlasnika <i>Etherum</i> povećao se 4,6 puta između januara i decembra 2023. godine.          |
| <b>Kripto za preduzeća</b>       | 36% malih preduzeća u Americi prihvatilo je kriptovalute u 2023. godini.                          |
| <b>Američki muški vlasnici</b>   | 88% vlasnika kriptovaluta u Americi u 2023. godini bili su muškarci.                              |
| <b>Prihodi</b>                   | U 2023. godini, 68,6% američkih vlasnika kriptovaluta koristilo je kripto za generisanje prihoda. |
| <b>Laundering (Pranje novca)</b> | Pranjem novca u kriptovalutama oprano je 8,88 milijardi dolara u 2023. godini.                    |
| <b>Nigerija</b>                  | Nigerija je predvodila u globalnim aktivnostima s kriptovalutama u 2023. godini.                  |

Digitalni novac i kriptovalute obuhvataju širok spektar finansijskih instrumenata prilagođenih savremenim tehnološkim potrebama. Centralizovani digitalni novac, poput *PayPal*-a i *Venmo*-a, funkcioniše pod nadzorom banaka i finansijskih institucija, pružajući sigurnost i regulativnu zaštitu korisnicima. Nasuprot tome, kriptovalute, kao što su *Bitcoin* i *Ethereum*, oslanjaju se na

decentralizovane mreže koje omogućavaju peer-to-peer transakcije bez posrednika. *Stablecoins*<sup>5</sup>, poput *Tethera* i *USD Coina*, predstavljaju most između tradicionalnog i digitalnog finansijskog sistema, nudeći stabilnost cena vezivanjem za fiat valute, uz prednosti brzih transakcija. Pored toga, digitalni tokeni imaju specifične funkcije unutar blokčejn projekata, omogućavajući vlasnicima pristup uslugama, glasanje ili ulaganje. Ovi različiti oblici digitalne imovine ne samo da redefinišu pojam novca, već i otvaraju vrata novim modelima poslovanja i finansijskih inovacija.

Digitalni novac i kriptovalute predstavljaju temelje budućnosti finansija. Dok digitalni novac omogućava efikasnost i sigurnost kroz centralizovane sisteme, kriptovalute nude slobodu, transparentnost i inovativnost kroz decentralizovane mreže. Kako globalna ekonomija postaje sve više digitalizovana, razumevanje ovih koncepata postaje ključno za oblikovanje modernih finansijskih sistema. Inovacije u bankarskim modelima nastavljaju da oblikuju novu paradigmu u kojoj finansijska dostupnost, sigurnost i brzina postaju standardi (Vives, 2019). Budućnost pripada onima koji se pripremaju za nju danas – uspon digitalnih finansija pokazuje da su tehnologije temelj ekonomskog napretka i društvene transformacije.

### 1.4.2 Onlajn plaćanja

Onlajn plaćanja predstavljaju ključnu komponentu savremenog finansijskog sistema, omogućavajući elektronski transfer novčanih sredstava između kupaca i prodavaca putem interneta. Ovaj proces uključuje niz sigurnosnih i tehničkih koraka – od unosa podataka o plaćanju, njihove enkripcije radi zaštite, do verifikacije transakcija i konačnog transfera sredstava. Digitalne tehnologije omogućavaju brze i efikasne transakcije bez potrebe za fizičkim prisustvom, čime se optimizuje poslovanje i unapređuje korisničko iskustvo (Doran, Bădîrcea, & Manta, 2022).

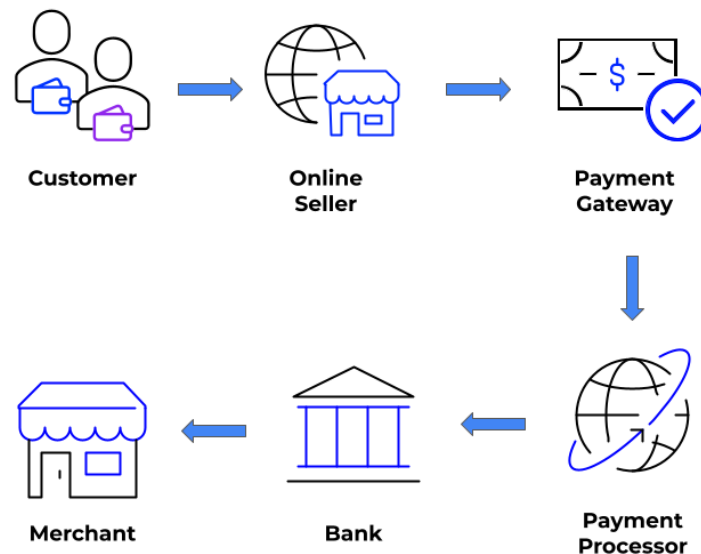
Slika 3. prikazuje proces onlajn plaćanja, ilustrujući ključne korake između kupca i trgovca. Prvo, kupac započinje transakciju kod onlajn prodavca, unoseći podatke o plaćanju. Zatim, informacije se šalju preko platnog prolaza, koji osigurava šifrovanje i verifikaciju podataka radi sigurnosti. Nakon toga, podaci se prosleđuju procesoru plaćanja koji komunicira s bankama kako bi

---

<sup>5</sup> Stablecoin je vrsta digitalne valute koja svoju vrednost veže za vrednost imovine poput zlata ili neke druge fiat valute kako bi održala stabilnost cene. Kombinacija stabilnosti koju nude tradicionalne valute i fleksibilnost digitalne imovine se pokazala kao popularna ideja među investitorima.

autorizovao transakciju. Banka proverava dostupnost sredstava i, ako je odobrena, sredstva se prebacuju trgovcu. Ovaj sistem osigurava brzinu, sigurnost i efikasnost transakcija, pružajući korisnicima jednostavno digitalno plaćanje.

Postoji nekoliko dominantnih vrsta onlajn plaćanja koje korisnicima nude fleksibilnost i sigurnost u transakcijama. Kreditne kartice omogućavaju kupovinu na kredit, dok debitne kartice direktno povlače sredstva sa tekućih računa. Popularne su i usluge trećih strana, poput *PayPal*-a i *Google Pay*-a, koje olakšavaju transakcije povezivanjem bankovnih računa kupaca i prodavaca (Häggqvist, 2019). Elektronski čekovi (engl. eChecks) predstavljaju digitalnu verziju papirnih čekova, dok bankovni transferi omogućavaju direktan prenos sredstava između računa, pružajući dodatnu sigurnost i brzinu.



Slika 3. Procedura onlajn plaćanja (Vives, 2019)

Ove metode pokrivaju različite potrebe tržišta, omogućavajući korisnicima globalno povezivanje.

Glavne prednosti onlajn plaćanja uključuju povećanu sigurnost kroz enkripciju podataka, brzinu obrade transakcija i eliminaciju geografskih ograničenja. Kupcima je omogućeno plaćanje u bilo koje vreme i sa bilo koje lokacije, čime se poboljšava njihovo iskustvo i povećava lojalnost prema trgovcima. Beskontaktne metode, poput QR kodova i jednokratnih lozinki, dodatno unapređuju bezbednost transakcija i smanjuju potrebu za fizičkim kontaktom, što je naročito važno u

postpandemijskom periodu (Hodula, 2022). Ove prednosti podstiču trgovce da sve više ulažu u digitalne platforme kako bi ostali konkurentni u dinamičnom poslovnom okruženju.

Razvoj onlajn plaćanja oslanja se na napredne softverske platforme i tehnologije koje podržavaju sigurne transakcije. Platni prolazni sistemi automatizuju plaćanja između kupaca i prodavaca, dok procesori plaćanja proveravaju validnost transakcija i odobravaju prenose sredstava. Instalacioni softver omogućava plaćanja na rate, dok analitički alati prate obrasce plaćanja i optimizuju poslovne procese. Softveri za izdavanje kartica kreiraju fizičke i virtuelne kartice, prilagođene specifičnim potrebama korisnika (Klein, 1971).

Onlajn plaćanja predstavljaju temelj modernih finansijskih sistema, omogućavajući kompanijama i pojedincima da odgovore na izazove digitalizacije i globalizacije. Njihova primena donosi efikasnost, smanjenje troškova i sigurnost, čime postaju ključni element savremenog poslovanja. Kako tehnologije poput veštačke inteligencije i blokčejn sistema nastavljaju da se razvijaju, očekuje se dalja evolucija onlajn plaćanja, otvarajući nove mogućnosti za unapređenje korisničkog iskustva i poslovnih procesa. Digitalna transformacija je, stoga, ne samo odgovor na trenutne potrebe tržišta, već i dugoročna strategija za održiv rast finansijskih institucija i trgovaca.

### **1.4.3 Plaćanja putem kartica i QR kodova**

Platne metode predstavljaju različite načine prenosa novca između kupaca i prodavaca prilikom kupovine roba i usluga. Njihova svrha je olakšavanje ekonomskih transakcija u fizičkom i digitalnom prostoru uz primenu različitih nivoa sigurnosti i pogodnosti. Savremeni platni sistemi omogućavaju brzo i efikasno obavljanje transakcija, bilo da su u pitanju tradicionalne metode poput gotovine ili inovativna rešenja poput digitalnih novčanika i kriptovaluta. Najzastupljeniji tipovi platnih metoda su (Elsaid, 2023):

- a) Debitne kartice – Omogućavaju direktno povlačenje sredstava sa bankovnog računa korisnika. Predstavljaju praktičan način plaćanja, ali su ograničene dostupnim sredstvima na računu. Njihova prednost je laka evidencija troškova, dok su slabosti manja zaštita u slučaju prevara i manjak pogodnosti poput nagradnih programa.

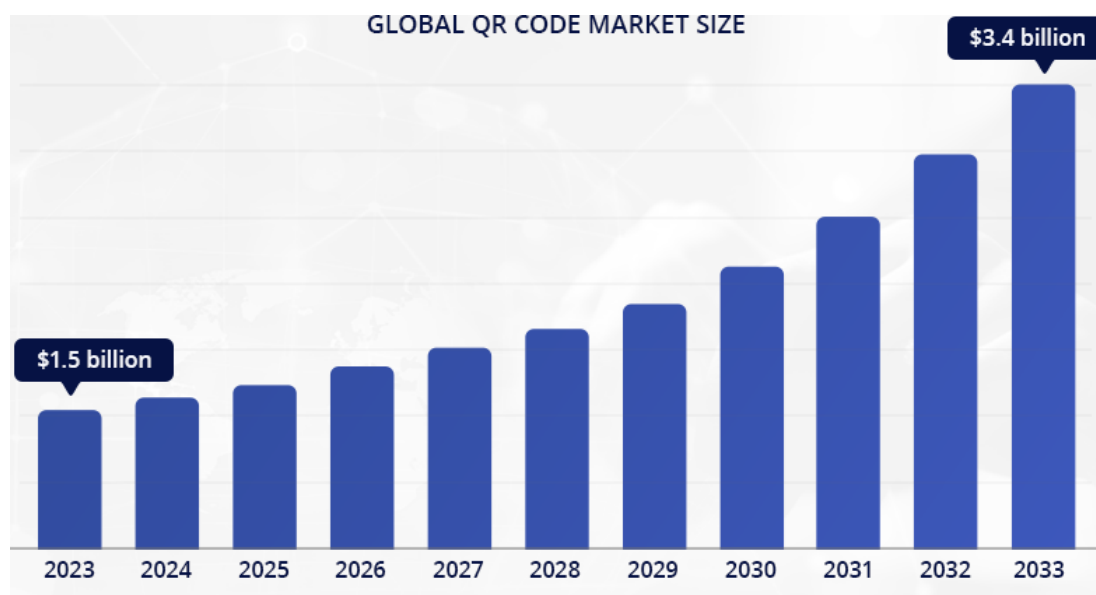
- b) Kreditne kartice – Nude fleksibilnost kroz odložena plaćanja i omogućavaju korisnicima da ostvaruju nagrade, povraćaj novca ili avionske milje.<sup>6</sup> Međutim, zbog mogućnosti nagomilavanja duga i visokih kamatnih stopa, zahtevaju pažljivo upravljanje. Njihova široka primena i zaštita od prevara čine ih poželjnom opcijom za globalna plaćanja.
- c) Prepaid kartice – Funkcionišu na principu unapred uplaćenih sredstava, čime se ograničava potrošnja na dostupni saldo. Idealne su za kontrolisano trošenje, ali često dolaze s dodatnim troškovima za aktivaciju i dopunu.
- d) Autoplaćanja (engl. Autopay) – Obezbeđuju automatsko plaćanje računa sa unapred podešenih bankovnih računa ili kreditnih kartica, čime se smanjuje rizik od kašnjenja plaćanja. Ipak, zahtevaju redovno praćenje stanja na računu kako bi se izbeglo prekoračenje limita.
- e) Gotovina – Tradicionalni način plaćanja, jednostavan i prihvaćen širom sveta, ali sa ograničenjima u pogledu sigurnosti i evidencije transakcija. Nije praktična za onlajn kupovine, što je čini manje popularnom u digitalnom dobu.
- f) Čekovi – Iako su klasična metoda plaćanja, koriste se sve ređe zbog sporog procesiranja i rizika od falsifikovanja. Njihova prednost je u jasnoj evidenciji transakcija i mogućnosti odloženih plaćanja.
- g) Kupovina sada, plaćanje kasnije (BNPL) – Sve popularnija metoda koja omogućava raspodelu plaćanja na rate bez kamata. Pogodna je za veću kupovinu, ali nosi rizik prekomerne potrošnje.
- h) NetBanking – Omogućava elektronske transfere između bankovnih računa. Ova metoda je brza i sigurna, ali zavisi od internet konekcije i podrške banke.
- i) Mobilna plaćanja – Korišćenje pametnih telefona za transakcije putem aplikacija ili QR kodova postaje sve popularnije. Nude visoku sigurnost kroz biometrijsku autentifikaciju, ali zahtevaju kompatibilnost uređaja i stabilnu konekciju.
- j) UPI i QR kodovi – Posebno popularni u azijskim zemljama, omogućavaju trenutno plaćanje putem mobilnih aplikacija i skeniranja kodova. Nude niski trošak transakcije i lakoću upotrebe, ali mogu biti podložni prevarama ako nisu adekvatno zaštićeni.

---

<sup>6</sup> Avionska milja je jedinica mere koja predstavlja rastojanje koje putnik prelazi tokom leta i koja se često koristi u programima lojalnosti avio-kompanija. Putnici sakupljaju milje prilikom letova i mogu ih kasnije iskoristiti za nagrade kao što su besplatne karte, nadogradnje sedišta ili druge pogodnosti. Jedna avionska milja obično odgovara jednoj pređenoj milji (1,609 km), ali uslovi zarade i korišćenja variraju u zavisnosti od programa.

k) POS terminali – Koriste se u fizičkim prodavnicama za plaćanje karticama. Brzi su i efikasni, ali zahtevaju posebnu opremu i tehničku podršku.

Plaćanje QR kodom omogućava beskontaktno transakcije putem mobilnih uređaja, kombinujući brzinu, sigurnost i jednostavnost, uz visoki nivo prihvatanja i široku upotrebu u različitim industrijama. U osnovi, QR kod je dvodimenzionalna matrica koja može sadržati informacije o primaocu, iznosu transakcije i dodatnim detaljima, čime omogućava automatsku obradu plaćanja. Popularnost ovog metoda značajno je porasla tokom pandemije, kada su beskontaktno opcije plaćanja postale prioritet zbog higijenskih i bezbednosnih razloga. Prema istraživanjima, digitalna transformacija finansijskog sektora ubrzala je primenu ovih tehnologija, posebno u zemljama Srednje i Istočne Evrope, gde su banke modernizovale svoje usluge kao odgovor na izazove pandemije (Doran et al., 2022).



Slika 4. Učešće na tržištu QR koda (Doran et al., 2022)

Proces plaćanja putem QR koda zasniva se na jednostavnom skeniranju koda putem kamere na pametnom telefonu. Kod sadrži ključne informacije, uključujući bankovne podatke primaoca i iznos transakcije. Nakon skeniranja, korisnik se preusmerava na stranicu za plaćanje gde potvrđuje podatke i završava transakciju unosom PIN-a ili korišćenjem biometrijske autentifikacije. Digitalna potvrda o uplati šalje se i kupcu i prodavcu, čime se proces završava za nekoliko sekundi. Ovakav model optimizuje transakcije u maloprodaji, ugostiteljstvu i e-trgovini, istovremeno

smanjujući redove i poboljšavajući korisničko iskustvo. Studije pokazuju da digitalna transformacija bankarskog sektora u Švedskoj već pruža slične benefite, integrišući moderne tehnologije radi poboljšanja operativne efikasnosti (Häggqvist, 2019). Slika 4. prikazuje rast globalnog tržišta QR kodova od 2023. godine, vrednog 1,5 milijardi dolara, do 2033. godine, kada se očekuje da dostigne 3,4 milijarde dolara, ukazujući na značajan porast usvajanja ove tehnologije.

Proces plaćanja je intuitivan i pristupačan korisnicima svih nivoa tehnološke pismenosti, dok skraćeno vreme transakcija povećava zadovoljstvo kupaca. Pored toga, dodatne mere bezbednosti poput enkripcije i tokenizacije smanjuju rizik od krađe podataka, dok dvofaktorska autentifikacija pruža dodatni sloj zaštite. QR kodovi omogućavaju i integraciju sa programima lojalnosti, čime se unapređuju marketinške strategije i povećava zadržavanje korisnika. U globalnom kontekstu, *fintech* sektor koristi slične inovacije kako bi proširio pristup kreditima i modernizovao finansijske usluge, dokazujući da digitalne alternative mogu zameniti tradicionalne metode zaduživanja (Hodula, 2022).

Generisanje QR kodova za plaćanje uključuje niz koraka koji osiguravaju funkcionalnost i bezbednost transakcija. Prvi korak podrazumeva izbor provajdera usluga koji podržava kreiranje kodova, nakon čega se unose podaci o transakciji, uključujući iznos, valutu i podatke o primaocu. Sistem zatim generiše jedinstveni kod koji se testira pre nego što postane dostupan za upotrebu. Kodovi se mogu postaviti na fakture, račune, mobilne aplikacije ili fizičke lokacije, čime postaju lako dostupni korisnicima. Ovakva fleksibilnost omogućava kompanijama da se prilagode rastućim potrebama digitalnog tržišta, povećavajući operativnu efikasnost i smanjujući troškove (Klein, 1971).

Bezbednost plaćanja putem QR koda obezbeđuje se naprednim tehnologijama poput enkripcije i tokenizacije, koje štite korisničke podatke od krađe. Sistem koristi više slojeva zaštite, uključujući biometrijsku autentifikaciju i dvofaktorsku verifikaciju, čime se značajno smanjuje rizik od zloupotreba. Međutim, korisnici moraju biti svesni mogućih pretnji, poput malicioznih kodova koji mogu sadržavati fišing (engl. phishing – pecanje) linkove ili preusmeravati na lažne stranice. Stoga je važno skenirati kodove samo iz proverenih izvora i redovno ažurirati bezbednosne postavke na mobilnim uređajima.

Najzad, plaćanje putem QR koda ne samo da pojednostavljuje proces transakcija, već pruža i dodatne funkcionalnosti poput praćenja podataka o kupovinama i analize potrošačkih navika. Njihova primena omogućava preduzećima da optimizuju strategije prodaje, integrišu programe lojalnosti i poboljšaju korisničko iskustvo. Kako digitalne tehnologije nastavljaju da evoluiraju, plaćanje putem QR koda će igrati ključnu ulogu u modernizaciji finansijskog sektora, pružajući sigurnu, efikasnu i prilagodljivu platformu za buduće transakcije.

#### **1.4.4 Digitalni novčanici**

Digitalni novčanici predstavljaju ključnu komponentu savremene digitalne ekonomije, omogućavajući korisnicima bezbedno skladištenje i upravljanje finansijskim podacima. Njihova funkcionalnost zasniva se na softverskim platformama koje integrišu metode plaćanja, lozinke i podatke o identifikaciji u jedan lako dostupan format. Zahvaljujući ovoj tehnologiji, korisnici mogu realizovati transakcije bez potrebe za fizičkim karticama ili gotovinom, čime se značajno unapređuje efikasnost i sigurnost finansijskih procesa.

Funkcionisanje digitalnih novčanika oslanja se na napredne tehnološke platforme koje koriste NFC (engl. Near Field Communication), QR kodove i magnetsku sigurnu transmisiju – MST (engl. Magnetic Secure Transmission). NFC omogućava bežični prenos podataka između uređaja na malim udaljenostima, dok QR kodovi funkcionišu kao vizuelni kodovi koji sadrže informacije o transakciji. MST emulira signal magnetne kartice, omogućavajući upotrebu digitalnih novčanika čak i na terminalima koji nisu opremljeni NFC tehnologijom. Ove metode ne samo da ubrzavaju proces plaćanja, već i minimizuju rizik od krađe podataka zahvaljujući naprednoj enkripciji.

Digitalni novčanici koriste mreže platnih procesora i sistema autentifikacije kako bi verifikovali transakcije u realnom vremenu. Ovaj pristup garantuje visok nivo sigurnosti i istovremeno omogućava brzinu obrade koja zadovoljava potrebe modernog tržišta. Studije o digitalnoj transformaciji bankarskog sektora, poput one sprovedene u Švedskoj, pokazuju da tehnološka prilagodljivost značajno doprinosi efikasnosti sistema plaćanja (Häggqvist, 2019).

Digitalni novčanici koriste naprednu enkripciju podataka i biometrijsku autentifikaciju, poput otiska prsta i prepoznavanja lica, kako bi obezbedili visoki nivo sigurnosti. Iako postoji rizik od

sajber napada i krađe podataka, kombinacija biometrijske autentifikacije i dvofaktorske verifikacije značajno smanjuje ove rizike (Mandic et al., 2014).

Digitalni novčanici igraju značajnu ulogu u inkluziji finansijskih usluga, posebno u nerazvijenim regijama. Njihova dostupnost putem mobilnih aplikacija omogućava ljudima bez bankovnih računa da učestvuju u savremenim ekonomskim tokovima. Ova pojava je posebno vidljiva u analizama digitalne ekonomije u Evropi, gde su istraživanja pokazala da digitalizacija doprinosi povećanju ekonomske konkurentnosti (Milošević et al., 2018).

Iako digitalni novčanici nude brojne benefite, suočavaju se i sa određenim izazovima. Ograničena prihvaćenost u ruralnim sredinama i manjim prodajnim objektima predstavlja prepreku za širu implementaciju. Takođe, zavisnost od internet konekcije i funkcionalnosti uređaja može uticati na njihovu dostupnost u situacijama kada tehnologija nije dostupna.

Digitalni novčanici i digitalna plaćanja postali su ključna komponenta globalnog finansijskog sistema, omogućavajući brže, sigurnije i efikasnije transakcije, dok njihova integracija sa kriptovalutama dodatno širi mogućnosti za međunarodne finansijske tokove (OECD, 2020; Vives, 2019). Predviđa se da će globalni prihod od digitalnih plaćanja dostići 14,79 biliona (engl. trillion) američkih dolara do 2027. godine, uz prosečnu godišnju stopu rasta od 11,79%, dok se očekuje da će u Sjedinjenim Američkim Državama premašiti 3,53 biliona dolara (PWC, 2016; OECD, 2020). Više od dve trećine odraslih osoba u svetu koristi digitalna plaćanja, a u razvijenim zemljama taj procenat dostiže i do 95% (Svetski ekonomski forum, 2018; Shahid et al., 2022). Poseban značaj ima rast e-trgovine, koja će do 2026. godine činiti 24% globalne potrošnje, pri čemu digitalni novčanici, poput PayPal-a, Apple Pay-a i Venmo-a, ostvaruju vodeću poziciju sa 49% udela u ukupnoj prodaji u SAD, gde je već 15% korisnika u potpunosti napustilo korišćenje fizičkih novčanika (PWC, 2016; Stefanovic et al., 2021). Istovremeno, čak 90% centralnih banaka širom sveta istražuje mogućnosti uvođenja digitalnih valuta, što dodatno potvrđuje značaj digitalizacije u savremenim finansijama (Fernández-Villaverde & Sanches, 2019). Međutim, i pored ovih napredaka, oko 1,4 milijarde odraslih osoba globalno i dalje nema pristup osnovnim bankarskim uslugama, što ukazuje na potrebu za razvojem inkluzivnih i pristupačnih digitalnih rešenja (Murinde et al., 2022).

Primeri iz prakse pokazuju da *fintech* rešenja, poput digitalnih novčanika, sve više zamenjuju tradicionalne bankarske usluge, pružajući brži pristup kreditima i plaćanjima (Hodula, 2022). Ova tranzicija ka digitalnim platformama otvara nova pitanja u vezi sa regulativama i zaštitom korisnika, što predstavlja ključne aspekte budućeg razvoja.

Razvoj digitalnih novčanika usmeren je na integraciju sa blokčejn tehnologijama i veštačkom inteligencijom, omogućavajući sigurnije i transparentnije transakcije. Pametni ugovori dodatno unapređuju sigurnost, dok analitika podataka omogućava personalizovane preporuke i optimizaciju potrošnje.

Predviđa se da će digitalni novčanici postati dominantno sredstvo plaćanja u narednim decenijama, a bankarski sektor će nastaviti da se prilagođava novim tehnologijama. Teorijski modeli koji analiziraju dinamiku bankarskih firmi potvrđuju da prilagođavanje inovacijama vodi ka većoj profitabilnosti i održivosti (Klein, 1971).

## **2 IZAZOVI I RIZICI DIGITALNIH TEHNOLOGIJA U BANKARSTVU**

Izazovi i rizici primene digitalnih tehnologija u bankarstvu postaju sve značajniji usled sveprisutne digitalizacije i rastuće zavisnosti finansijskog sektora od informacionih sistema. Ova transformacija, iako donosi brojne prednosti u pogledu efikasnosti i dostupnosti usluga, istovremeno otvara prostor za nove bezbednosne pretnje i tehničke slabosti. Bezbednost digitalnog novca i kriptovaluta suočava se sa pretnjama kao što su sajber napadi, krađa digitalnog identiteta i hakerski upadi u blokčejn mreže. Regulatorne prepreke, uključujući neujednačenu zakonsku regulativu i složenost međunarodnog usklađivanja, dodatno komplikuju proces digitalne tranzicije. Posebni izazovi javljaju se i u oblasti onlajn plaćanja i elektronskih transakcija, gde su brzina i obim obrade podataka često u neskladu sa nivoima zaštite koji su potrebni. Zbog toga banke razvijaju sofisticirane strategije za sprečavanje prevara i zaštitu podataka, oslanjajući se na napredne sisteme enkripcije, višefaktorsku autentifikaciju i usklađenost sa propisima poput Opšte uredbe o zaštiti podataka (GDPR), čime se nastoji očuvati integritet digitalnog finansijskog sistema.

### **2.1 Bezbednost digitalnog novca i kriptovaluta**

Bezbednost digitalnog novca i kriptovaluta oslanja se na složene sigurnosne arhitekture koje obuhvataju hardverske, softverske i proceduralne komponente. Ključna tehnologija u ovom kontekstu je blokčejn, koji se koristi za obezbeđivanje transakcija, čuvanje podataka i kontrolu pristupa, stvarajući pouzdan i decentralizovan sistem razmene.

#### **2.1.1 Arhitektura bezbednosti**

Sigurnosna arhitektura digitalnog novca uključuje tri glavna sloja zaštite. Prvi sloj čini infrastruktura koja obuhvata fizičke uređaje, servere, mreže i skladišta podataka. Drugi sloj predstavlja mrežna zaštita, koja omogućava šifrovanu komunikaciju između korisnika i sistema, uključujući autentifikaciju i zaštitu od mrežnih napada. Treći sloj je aplikativni, koji obezbeđuje korisnički pristup i upravljanje transakcijama putem platformi i aplikacija. Ove komponente funkcionišu kao celina kako bi garantovale dostupnost, integritet i poverljivost podataka.

Blokčejn tehnologija predstavlja distribuiranu bazu podataka koja beleži sve transakcije u formi blokova povezanih kriptografskim algoritmima. Ova struktura omogućava transparentnost i nepromenljivost jer jednom zabeležene transakcije ne mogu biti izmenjene, čime se eliminiše mogućnost falsifikovanja podataka. Decentralizacija podataka dodatno smanjuje rizik od napada, a konsenzus algoritmi, poput *Proof-of-Work* (PoW)<sup>7</sup> i *Proof-of-Stake* (PoS)<sup>8</sup>, osiguravaju validaciju transakcija i sprečavaju duplo trošenje (engl. double spending). Primer *Bitcoin* kao najpoznatije kriptovalute pokazuje kako blokčejn eliminiše posrednike i smanjuje troškove transakcija, uz garantovanu bezbednost (Stefanovic et al., 2021).

Blokčejn mreže mogu se podeliti prema nivou pristupa. Javne mreže, poput *Bitcoin* i *Etherum*, otvorene su za sve korisnike, dok su privatne mreže ograničene na ovlašćene korisnike, što ih čini pogodnim za korporativne aplikacije. Konzorcijske mreže kombinuju javne i privatne karakteristike, omogućavajući kontrolisanu transparentnost. Privatne i hibridne mreže sve češće se razmatraju kao platforme za centralnobankarske digitalne valute (CBDC) zbog bolje usklađenosti sa regulatornim zahtevima (Vives, 2019).

Alternativni algoritmi, poput *Proof-of-Burn*<sup>9</sup>, omogućavaju „sagorevanje” kriptovaluta radi validacije blokova, smanjujući energetske troškove. Ovi algoritmi smanjuju mogućnost napada na mrežu i obezbeđuju sigurnost podataka (Ekinci, 2021).

Centralne banke razmatraju primenu blokčejna za kreiranje digitalnih valuta (CBDC), ističući prednosti kao što su transparentnost, otpornost na prevare i regulatorna kontrola. Međutim, ograničenja u skalabilnosti i interoperabilnosti blokčejna predstavljaju izazove za punu implementaciju CBDC sistema (Do, Pham, Thalassinou, & Le, 2022). Distribuirane knjige (engl. Distributed Ledger Technology – DLT) dodatno unapređuju bezbednost, omogućavajući decentralizovanu kontrolu, P2P validaciju i otpornost na manipulacije (Baskerville, Capriglione,

---

<sup>7</sup> *Proof-of-Work* je konsenzus algoritam koji koristi složene matematičke probleme kako bi validirao transakcije i dodao nove blokove u blokčejn. Ovaj mehanizam zahteva značajnu računarsku snagu, ali garantuje sigurnost sistema.

<sup>8</sup> *Proof-of-Stake* funkcioniše tako što korisnici ulažu (engl. stake) svoje kriptovalute kako bi učestvovali u validaciji transakcija. Ovaj pristup smanjuje energetske troškove u poređenju sa PoW metodom.

<sup>9</sup> *Proof-of-Burn* je tehnički pojam koji se koristi u oblasti kriptovaluta za opisivanje procesa dokazivanja vlasništva ili angažovanja resursa kroz sagorevanje (uništavanje) tokena ili sredstava. U ovom kontekstu, korisnici uništavaju određeni iznos tokena kako bi dobili poboljšane privilegije ili nagrade unutar ekosistema.

& Casalino, 2020). DLT<sup>10</sup> se sve više koristi u aplikacijama za digitalne identitete, finansijske transakcije i IoT sisteme.

Iako blokčejn pruža visok nivo zaštite, postoje određeni izazovi. Napadi dvostruke potrošnje, anonimnost korisnika i slabosti softverskog koda predstavljaju potencijalne pretnje. Rešenja uključuju napredne metode šifrovanja, algoritme za otkrivanje pretnji i redovno ažuriranje sistema. Posebno je važno obezbediti višeslojnu zaštitu, uključujući infrastrukturu, mrežnu bezbednost i aplikativne sisteme kako bi se garantovala pouzdanost sistema (Budler, Župič, & Trkman, 2021).

Bezbednost digitalnog novca i kriptovaluta zasniva se na naprednim sigurnosnim arhitekturama koje integrišu blokčejn tehnologiju, distribuirane knjige i konsenzus algoritme. Ove tehnologije pružaju visok nivo zaštite podataka i transparentnosti, ali se suočavaju sa izazovima kao što su skalabilnost i energetska efikasnost. Dalje inovacije u oblasti blokčejna i DLT-a ključne su za unapređenje sigurnosti digitalnih finansijskih sistema u budućnosti (Elsaid, 2023).

### **2.1.2 Modeli bezbednosti: ključne komponente i primena u kriptovalutama**

Modeli bezbednosti predstavljaju formalne okvire koji definišu pravila zaštite u informacionim sistemima, oslanjajući se na tri osnovna principa: poverljivost, integritet i dostupnost – poznate kao CIA (engl. Confidentiality, Integrity, Availability) trijada. Ovaj model se široko primenjuje u cilju očuvanja bezbednosti podataka, posebno u kontekstu digitalnih valuta i kriptovaluta.

Poverljivost se odnosi na zaštitu informacija od neovlašćenog pristupa i objavljivanja. U oblasti digitalnog novca, ovo podrazumeva čuvanje privatnih ključeva i zaštitu transakcija od neautorizovanih lica. Na primer, kriptografski ključevi u kriptovalutama igraju ključnu ulogu u očuvanju identiteta korisnika. Najbolja praksa uključuje upotrebu višefaktorske autentifikacije, kao i korišćenje multi-potpis (engl. multi-signature) sistema kako bi se smanjio rizik od krađe ili zloupotrebe ključeva. Neslavni slučaj Mt. Gox<sup>11</sup>, u kojem je zbog slabe zaštite izgubljeno više miliona dolara u Bitkoinima, naglašava važnost ovih mera zaštite. Kriptovalute koriste šifrovanje

---

<sup>10</sup> DLT tehnologija omogućava decentralizovano vođenje evidencija o transakcijama, smanjujući potrebu za posrednicima i povećavajući transparentnost.

<sup>11</sup> Mt. Gox, jedna od prvih i najvećih berzi za trgovinu Bitkoinom, pretrpela je hakerski napad zbog loših bezbednosnih mera, pri čemu je izgubljeno 850.000 Bitkoina. Ovaj incident je naglasio potrebu za jačim sigurnosnim protokolima u kripto-industriji.

i decentralizovane mreže zasnovane na blokčejn tehnologiji kako bi obezbedile poverljivost podataka. Međutim, korisnici snose odgovornost za održavanje sigurnosti svojih privatnih ključeva, što uključuje zaštitu od neovlašćenih pristupa, ali i od nepažljivog rukovanja podacima (Doran et al., 2022).

Integritet se odnosi na tačnost, konzistentnost i celovitost podataka. U kontekstu blokčejna, transakcije su nepromenljive nakon što budu verifikovane i zapisane u blok. Ovaj proces omogućava zaštitu podataka od izmena i falsifikovanja, pružajući transparentnost i pouzdanost. Blokčejn osigurava integritet koristeći kriptografske algoritme i decentralizovane konsenzus mehanizme, kao što su *Proof-of-Work* (PoW) i *Proof-of-Stake* (PoS). Ipak, blokčejn ne može da ispravi greške pri unosu podataka, što potvrđuje princip „*garbage in, garbage out*” – loši podaci ostaju trajno zabeleženi u lancu. Stoga je od ključne važnosti sprovesti rigorozne mere unosa i validacije podataka kako bi se očuvao integritet sistema. Korisnici kriptovaluta moraju da preduzmu dodatne mere zaštite, poput kreiranja jedinstvenih adresa za svaku transakciju i skladištenja ključeva na sigurnim lokacijama. U slučaju gubitka ključeva, pristup sredstvima postaje nemoguć, što ukazuje na značaj pravilnog upravljanja identitetima i podacima (Häggqvist, 2019).

Dostupnost podrazumeva osiguravanje pristupa podacima i sistemima ovlašćenim korisnicima u svakom trenutku. U sistemima digitalnog novca, ovo je ključno za pružanje usluga transakcija i upravljanja sredstvima u realnom vremenu. Visoka dostupnost postiže se primenom mehanizama zaštite, kao što su sigurnosne kopije podataka, agregacija mrežnih komponenti i zaštita od DDoS (engl. Distributed Denial of Service) napada. U oblasti kriptovaluta, decentralizovana priroda blokčejna omogućava otpornost na prekide sistema, jer ne postoji jedinstvena tačka kvara. Međutim, hakerski napadi na digitalne novčanike i berze ukazuju na potrebu za dodatnim mehanizmima zaštite, uključujući multifaktorsku autentifikaciju i šifrovanje (Hodula, 2022). Sistem kontrole pristupa igra ključnu ulogu u očuvanju dostupnosti i sprečavanju neovlašćenih radnji. Upravljanje pravima korisnika i definisanje uloga unutar sistema dodatno smanjuju rizik od zloupotrebe podataka i transakcija.

Iako je CIA trijada osnova informacionih bezbednosnih sistema, njena primena u digitalnim valutama suočava se s izazovima. Kritičari ističu da model ne uzima u obzir društvene i

organizacione faktore bezbednosti, poput socijalnog inženjeringa i ljudskih grešaka, koje su česti uzroci bezbednosnih incidenata (Klein, 1971). Pored toga, eksplozivan rast prevara i hakovanja u svetu kriptovaluta ukazuje na potrebu za dodatnim slojevima zaštite, kao što su dinamičke politike pristupa, proaktivno praćenje pretnji i napredni algoritmi za detekciju anomalija. Dalji razvoj modela uključuje integraciju sa veštačkom inteligencijom i mašinskim učenjem, koji omogućavaju brzo prepoznavanje i reagovanje na potencijalne pretnje. Uvođenje blokčejn tehnologije u sisteme digitalnih valuta, uključujući centralnobankarske digitalne valute, otvara nove mogućnosti za unapređenje bezbednosti, ali zahteva detaljnu analizu skalabilnosti i regulatornih izazova.

### 2.1.3 Sigurni metodi prenosa podataka

Blokčejn tehnologija je prepoznata kao dominantna tehnologija u svetu digitalnih valuta i kriptovaluta. Najveće i najpoznatije kriptovalute, kao što su *Bitcoin* i *Ethereum*, implementirane su na ovoj tehnologiji, dok se mnoge druge, poput *Litecoin* i *Deuterium*, takođe oslanjaju na blokčejn. Osim u finansijskom sektoru, blokčejn se koristi i u oblastima kao što su pametne mreže, zdravstvena zaštita, telemedicina, osiguranje i energetske mreže. Njegova primena obuhvata i skladištenje podataka, računarstvo u oblaku, bežične mreže senzora, trgovinu energetskim ugovorima i prenose uživo (PWC, 2016).

Blokčejn omogućava razmenu vrednih digitalnih sredstava kroz visoko bezbedne mehanizme. Njegova sigurnosna arhitektura zasniva se na decentralizaciji, nepromenljivosti podataka i transparentnosti (Osterwalder et al., 2005). Blokčejn koristi kriptografske funkcije kao osnovu za zaštitu podataka. Najpoznatiji algoritmi su SHA-256 (*Bitcoin*) i Keccak256 (*Ethereum*), koji obezbeđuju otpornost na kolizije i nemogućnost vraćanja ulaznih podataka iz heš vrednosti. Struktura podataka zasniva se na Merkle stablima koja omogućavaju proveru integriteta transakcija i osiguravaju da preneti blokovi podataka nisu oštećeni (Shahid et al., 2022). Osim toga, parovi javnih i privatnih ključeva generišu se pomoću algoritama kao što su ECDSA<sup>12</sup> i RSA<sup>13</sup>, čime se garantuje autentičnost korisnika i transakcija (Pavithra & Geetha, 2021).

---

<sup>12</sup> ECDSA (engl. Elliptic Curve Digital Signature Algorithm) je kriptografski algoritam koji Bitcoin koristi kako bi osigurao da sredstva mogu da troše samo njihovi zakoniti vlasnici.

<sup>13</sup> RSA (engl. Rivest-Shamir-Adleman) je kriptosistem sa javnim ključem koji koristi par ključeva za obezbeđivanje digitalne komunikacije i transakcija preko nebezbednih mreža, kao što je internet.

Uprkos visokim standardima bezbednosti, blokčejn sistemi suočavaju se sa izazovima, uključujući probleme skalabilnosti, zaštite privatnosti korisnika i potrošnje energije (Revathi, 2019). Rešenja uključuju hibridne metode enkripcije, kao što su simetrična lozinka kombinovana s asimetričnim ključevima, kao i implementaciju protokola nultog znanja (engl. Zero Knowledge Proof)<sup>14</sup> radi anonimizacije korisnika. Osim toga, tehnologije poput *InterPlanetary File System* (IPFS)<sup>15</sup> i *BigChainDB*<sup>16</sup> nude mogućnosti za povećanje kapaciteta obrade podataka, čime se prevazilaze skalabilni problemi javnih blokčejna (Sayed & Sayed, 2020).

Brzina obrade transakcija takođe predstavlja izazov. Na primer *Ripple* (XRP) omogućava potvrdu transakcija za oko 5 sekundi, dok *Bitcoin* zahteva oko 10 minuta. Ovo ukazuje na potrebu za optimizacijom algoritama u procesima rudarenja, prenosa ključeva i izvršenja pametnih ugovora, pri čemu se dodatno smanjuje energetska potrošnja (Häggqvist, 2019).

Istraživači predlažu i primenu metoda baziranih na teoriji igara kako bi se osigurala pravedna validacija transakcija i smanjili problemi sebičnog ponašanja korisnika. Ove metode nagrađuju korisnike koji doprinose uspešnim transakcijama, čime se podstiče stabilnost sistema i minimizuju sigurnosni rizici (Budler et al., 2021).

Blokčejn tehnologija, kroz decentralizaciju i kriptografske funkcije, omogućava visoke standarde bezbednosti podataka i transakcija, ali njena praktična implementacija zahteva stalna unapređenja zbog skalabilnosti, energetske efikasnosti i privatnosti.<sup>17</sup> Dalje inovacije, poput konsenzus algoritama i distribuiranih knjiga (DLT), ključne su za održavanje pouzdanosti ovih sistema u različitim aplikacijama (Do et al., 2022). Sigurni metodi prenosa podataka, koji kombinuju kriptografsku zaštitu i decentralizovanu kontrolu, osiguravaju zaštitu digitalnih valuta i osnažuju poverenje korisnika u moderne finansijske sisteme.

---

<sup>14</sup> Protokol nultog znanja (ZKP) omogućava dokazivanje posedovanja određenih informacija bez otkrivanja samih informacija. Ova tehnologija se često koristi za zaštitu privatnosti u kriptovalutama.

<sup>15</sup> IPFS je distribuirani sistem za skladištenje i deljenje podataka koji omogućava povećanu skalabilnost i sigurnost u poređenju sa tradicionalnim centralizovanim serverima.

<sup>16</sup> BigChainDB je unapređena blokčejn baza podataka. Dizajnirana je da spoji najbolje od oba sveta: tradicionalnog sveta distribuiranih baza podataka i tradicionalnog sveta blokčejna.

<sup>17</sup> Blokčejn tehnologija obezbeđuje transparentnost i otpornost na manipulacije. Banke kao što su Santander i JP Morgan, već su implementirale blokčejn za međunarodna plaćanja, potvrđujući njegovu efikasnost i sigurnost.

## 2.2 Regulatorni izazovi u primeni digitalnih tehnologija u bankarstvu

Regulatori širom sveta suočavaju se sa izazovom postizanja ravnoteže između podsticanja inovacija u digitalnom bankarstvu i zaštite potrošača od potencijalnih rizika. Dok, većina zemalja primenjuje postojeće bankarske zakone i propise na digitalne startupove i *fintech* kompanije, pojedine jurisdikcije, poput Singapura i Malezije, razvile su posebne regulatorne okvire prilagođene digitalnom bankarstvu. Ovi okviri ne samo da osiguravaju stabilnost i bezbednost sistema već podržavaju i šire političke ciljeve, poput povećanja finansijske inkluzije i podsticanja konkurencije u specifičnim segmentima tržišta. Takav pristup omogućava digitalnim bankama lakši ulazak na tržište i istovremeno postavlja jasne standarde za upravljanje rizicima i zaštitu korisnika, čime se stvara osnova za održiv rast i razvoj digitalnog finansijskog ekosistema.

Digitalno bankarstvo postalo je prisutno širom sveta, omogućavajući korisnicima brze i efikasne finansijske usluge kroz tradicionalne banke, *fintech* kompanije i potpuno digitalne banke. Iako je ovaj poslovni model relativno nov, regulatorni organi širom sveta razvili su specifične licence kako bi kontrolisali njegov razvoj i rizike. U Kini, digitalne banke poput WeBank i MYbank, koje podržavaju tehnološki giganti Tencent i Alibaba, uspele su da privuku milione korisnika u kratkom vremenskom roku. WeBank opslužuje preko 200 miliona ljudi, dok MYbank nudi usluge za više od 20 miliona malih i srednjih preduzeća (SME). Njihov uspeh naglašava potencijal digitalnog bankarstva u povećanju finansijske inkluzije i podrške malim preduzećima. Slično tome, južnokorejska KakaoBank je privukla više od deset miliona korisnika u prvoj godini poslovanja i prikupila 2,3 milijarde dolara kroz inicijalnu javnu ponudu u 2021. godini (Häggqvist, 2019).

### 2.2.1 Digitalno bankarstvo danas

Uspeh digitalnih banaka u velikoj meri zavisi od regulatornih okvira i tehnoloških inovacija koje omogućavaju njihovu integraciju u finansijski sektor. Ključni regulatorni alati uključuju elektronsku identifikaciju (engl. e-KYC), e-potpis i otvoreno bankarstvo (engl. open banking). Elektronska identifikacija omogućava digitalno otvaranje računa uz analitičke provere identiteta i sprečavanje pranja novca. Na primer, Velika Britanija je razvila sisteme koji podržavaju e-KYC za brzo verifikovanje identiteta, dok Kina koristi biometrijske podatke kao dodatnu meru bezbednosti (Hodula, 2022).

Otvoreno bankarstvo omogućava deljenje finansijskih podataka između banaka i trećih strana, čime se podstiče konkurencija i inovacije. Ova praksa je podržana regulativom PSD2 u Evropskoj uniji, koja olakšava integraciju finansijskih usluga i omogućava razvoj personalizovanih rešenja za korisnike. *Cloud hosting* dodatno smanjuje troškove infrastrukture i omogućava fleksibilnost u skladu sa lokalnim propisima o čuvanju podataka. Studija (Klein, 1971) naglašava važnost fleksibilnosti i efikasnosti u pružanju finansijskih usluga, što su ključni elementi digitalnog bankarstva danas.

Digitalne banke su često fokusirane na specifične niše i koriste tehnološke inovacije za pružanje prilagođenih usluga. Na primer, kineski aiBank, zajednički projekat CITIC Banke i tehnološke kompanije Baidu, nudi finansijska rešenja mladima i mikropreduzećima u ruralnim područjima. PAO Bank u Hong Kongu pruža brze kredite malim i srednjim preduzećima, dok Telenor Microfinance Bank u Pakistanu pruža digitalne finansijske usluge stanovništvu bez pristupa tradicionalnim bankarskim sistemima. Ovi modeli pokazuju kako digitalno bankarstvo može proširiti finansijsku inkluziju i omogućiti pristup kreditima za prethodno zapostavljene grupe korisnika.

Studije poput one koju je sproveo (Häggqvist, 2019) potvrđuju da digitalna transformacija omogućava bankama da postanu efikasnije i konkurentnije. Takođe, rad (Hodula, 2022) pokazuje da *fintech* krediti mogu biti održiva alternativa tradicionalnim kreditnim institucijama, posebno u ekonomijama u razvoju. Studija (Klein, 1971) ističe važnost optimizacije operacija u bankarskom sektoru, što se postiže kroz integraciju digitalnih tehnologija i regulatornih inovacija.

## **2.2.2 Licenciranje digitalnih banaka i regulatorni pristupi**

Razvoj digitalnog bankarstva širom sveta podstakao je regulatore da usvoje različite modele licenciranja kako bi podržali inovacije, povećali finansijsku inkluziju i obezbedili stabilnost finansijskih sistema. Ovi pristupi balansiraju između podsticanja konkurencije i zaštite potrošača, istovremeno smanjujući rizike koji mogu ugroziti poverenje u finansijski sektor (Milosevic et al., 2021).

Postoje dva glavna modela licenciranja digitalnih banaka. Prvi model uključuje specifične licence za digitalne banke, koje su usvojile zemlje poput Kine, Hong Konga, Singapura i Južne Koreje.

Ove licence preciziraju dozvoljene proizvode, ciljne korisnike i fizičko prisustvo, čime omogućavaju postepeni razvoj digitalnih banaka. Na primer, Južna Koreja je omogućila KakaoBank-u da odmah nudi širok spektar usluga, dok je Singapur uveo ograničenja na depozite u početnoj fazi kako bi postepeno kontrolisao njihov rast (Khuong et al., 2022).

Drugi model se oslanja na tradicionalne bankarske licence, koje omogućavaju digitalnim bankama da započnu sa ograničenim licencama, poput onih za e-plaćanja, pre nego što prošire svoje usluge. Primeri uključuju NuBank u Brazilu, koji je 2018. godine dobio licencu za maloprodajne usluge, i Revolut u Velikoj Britaniji, koji je svoju punu bankarsku licencu dobio tek 2018. godine kroz Litvaniju (OECD, 2020).

Azijske zemlje, poput Singapura i Malezije, prednjače u uvođenju specifičnih licenci, fokusirajući se na finansijsku inkluziju i podršku malim i srednjim preduzećima (MSP - engl. SME). Malezija je, na primer, postavila ograničenja na početni kapital kako bi omogućila manjim igračima da uđu na tržište, dok su Kina i Južna Koreja dozvolile potpunu ponudu proizvoda od samog početka (Murinde et al., 2022).

Evropska unija i SAD, s druge strane, oslanjaju se na postojeće bankarske licence uz prilagođene propise za digitalna rešenja. Direktiva PSD2 u EU omogućila je razvoj otvorenog bankarstva, dok su SAD uvele postepeni pristup licenciranju, pri čemu digitalne banke započinju sa e-plaćanjima pre nego što dobiju punu licencu (Milošević et al., 2018).

Regulatori ne samo da izdaju licence, već i oblikuju tržišne uslove koji podstiču inovacije i smanjuju rizike. Postavljanjem standarda za API (engl. Application Programming Interface) protokole i otvoreno bankarstvo, regulatori omogućavaju efikasnije upravljanje podacima i procenu rizika. Takođe, *sandbox* modeli, poput onih u Singapuru i Velikoj Britaniji, omogućavaju testiranje novih tehnologija u kontrolisanim uslovima, čime se smanjuju regulatorne nesigurnosti (Khuong et al., 2022).

Regulatorni okviri za digitalno bankarstvo igraju ključnu ulogu u balansiranju između podsticanja inovacija i zaštite stabilnosti finansijskog sistema. Prema (Ekinci, 2021), digitalizacija u finansijskom sektoru značajno je unapredila performanse banaka kroz efikasnije procese, smanjenje troškova transakcija i povećanu dostupnost usluga. Njegova analiza ukazuje da

implementacija digitalnih tehnologija može povećati produktivnost banaka za 15–20% u prvoj godini primene, čime se dodatno jača konkurentnost sektora.

U radu (Elsaid, 2023) se naglašava da *fintech* kompanije, kao glavni pokretači digitalizacije, vrše pritisak na tradicionalne banke da modernizuju svoje sisteme i usluge. Njegova studija ističe da su *fintech* inovacije, poput mobilnog bankarstva, digitalnih novčanika i blokčejn tehnologija, postale ključni faktori rasta digitalnog bankarstva. Na primer, *fintech* platforme omogućile su brzo odobravanje kredita i unapređeno praćenje transakcija, čime su smanjile vreme obrade zahteva za 40%. Ovi podaci pokazuju kako konkurencija podstiče banke da integrišu nove tehnologije i poboljšaju kvalitet usluga.

Pandemija COVID-19 dodatno je ubrzala digitalizaciju finansijskog sektora, posebno u Srednjoj i Istočnoj Evropi. U radu (Doran, Bădîrcea, & Manta, 2022) se navodi da su digitalne platforme tokom pandemije omogućile nesmetano poslovanje banaka, uprkos fizičkim ograničenjima. Prema njihovim podacima, onlajn transakcije u ovom periodu porasle su za 65%, dok je upotreba digitalnih kanala za upravljanje računima skočila za 45%. Ovi podaci potvrđuju da je digitalizacija ključna za otpornost finansijskog sistema u kriznim situacijama.

U kontekstu ovih nalaza, regulatorni okviri postaju sve značajniji za očuvanje sigurnosti i stabilnosti digitalnog bankarstva. Rad (Ekinci, 2021) ističe potrebu za jačim propisima koji regulišu sajber bezbednost, dok (Elsaid, 2023) naglašava važnost zaštite potrošača kroz transparentnost algoritama i veštačke inteligencije (AI). Ove studije ukazuju na to da pravilno usklađeni zakonski okviri, poput EU regulative DORA (engl. Digital Operational Resilience Act) i MiCA (engl. Markets in Crypto-Assets Regulation), omogućavaju dalji razvoj digitalnog bankarstva uz minimizaciju rizika.

### **2.2.3 Izazovi u primeni regulative**

Jedan od najvećih regulatornih izazova odnosi se na balans između podsticanja inovacija i zaštite potrošača. Regulatorni okviri moraju omogućiti razvoj digitalnih rešenja, ali i osigurati kontrolu rizika.

Zakon o digitalnoj operativnoj otpornosti (DORA) predstavlja ključni korak ka unapređenju sigurnosti informaciono-komunikacionih sistema u finansijskom sektoru Evropske unije. Njegov

primarni cilj je zaštita od sajber napada, operativnih prekida i tehnoloških kvarova koji mogu ugroziti stabilnost sistema. Prema podacima Evropske agencije za sajber bezbednost (ENISA), broj sajber-napada na finansijske institucije u EU porastao je za 38% između 2020. i 2023. godine, što ukazuje na hitnu potrebu za regulativom koja će minimizirati rizike. DORA uvodi obavezu finansijskim institucijama da sprovedu redovne stres-testove sistema, koriste napredne metode enkripcije i imaju procedure za upravljanje incidentima. Statistika izveštaja Evropske centralne banke (ECB) pokazuje da je 92% finansijskih institucija u EU, već implementiralo osnovne mere digitalne zaštite, dok je 48% započelo dodatne investicije u unapređenje digitalne otpornosti u skladu sa zahtevima DORA regulative. Očekuje se da će ove mere, kada budu u potpunosti primenjene 2025. godine, smanjiti rizik od sajber incidenata za 65%, čime će se povećati poverenje korisnika u digitalne finansijske usluge.<sup>18</sup>

Pravila o tržištima krypto-imovine (MiCA) stupila su na snagu u junu 2023. godine i obuhvataju širok spektar finansijskih proizvoda zasnovanih na blokčejn tehnologiji. Njihova svrha je pružanje regulatornog okvira za krypto-imovinu, uz istovremeno podsticanje inovacija i zaštitu investitora. Prema podacima Evropskog tržišnog tela za hartije od vrednosti, vrednost tržišta krypto-imovine u EU dostigla je 1,2 milijarde evra u 2023. godini, dok je broj korisnika kriptovaluta porastao za 28% u odnosu na prethodnu godinu. MiCA reguliše elektronske novčane tokene i tokene referencirane na imovinu, koji čine više od 70% ukupnog prometa krypto-imovine u EU. Posebna pažnja posvećena je stabilnim kriptovalutama, s obzirom na to da su one prepoznate kao potencijalna pretnja za monetarnu politiku i finansijsku stabilnost. Na primer, analiza ECB-a pokazuje da bi neuređena tržišta stabilnih valuta mogla povećati rizik od špekulativnih balona za 45%. Implementacija MiCA regulative omogućava transparentnost u trgovanju, zaštitu investitora kroz obavezne bele knjige sa detaljima o tokenima i postavljanje jasnih pravila za pružaoce usluga. Predviđa se da će MiCA doprineti smanjenju regulatornih nesigurnosti za 40% do kraja 2025. godine, čime će se podstaći dalji razvoj tržišta krypto-imovine u EU.<sup>19</sup>

Plan uvođenja digitalnog evra od strane Evropske centralne banke (ECB) predstavlja odgovor na brzi rast upotrebe digitalnih valuta i potrebu za očuvanjem monetarnog suvereniteta EU. Prema

---

<sup>18</sup> [https://www.eiopa.europa.eu/digital-operational-resilience-act-dora\\_en](https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en)

<sup>19</sup> <https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica>

podacima ECB-a, više od 55% građana EU već koristi digitalna sredstva plaćanja, dok je upotreba gotovine opala za 35% u poslednjih deset godina. Digitalni evro planiran je kao elektronski oblik centralnobankarskog novca, koji će funkcionisati paralelno sa fizičkim evrom. Njegova uloga je obezbeđenje brzih i sigurnih transakcija, kako na nacionalnom, tako i na prekograničnom nivou. ECB predviđa da bi digitalni evro mogao smanjiti troškove transakcija za 10–15% u odnosu na postojeće elektronske sisteme, dok bi interoperabilnost sa privatnim platnim platformama omogućila dodatnu efikasnost. Uvođenje digitalnog evra takođe bi povećalo finansijsku inkluziju, jer bi omogućilo pristup finansijskim uslugama osobama bez bankarskih računa, kojih prema podacima Evropske komisije ima oko 13,5 miliona u EU. Prema najnovijim informacijama Evropske centralne banke (ECB), projekat digitalnog evra je ušao u pripremnu fazu koja traje od novembra 2023. do oktobra 2025. godine. Tokom ovog perioda, ECB se fokusira na finalizaciju pravila sistema, izbor pružalaca usluga, eksperimentisanje i dalje tehničko istraživanje, uključujući razvoj funkcionalnosti za oflajn plaćanja. Planirano je da od novembra 2025. godine započne razvoj i implementacija konkretnih slučajeva upotrebe digitalnog evra. Međutim, konačna odluka o izdavanju digitalnog evra biće doneta tek nakon završetka zakonodavnog procesa u Evropskoj uniji. Dakle, i dalje se očekuje da će prve probe digitalnog evra započeti 2025. godine, a njegova šira primena mogla bi uslediti do 2030. godine, u zavisnosti od napretka u zakonodavnom okviru i tehničkoj pripremi.<sup>20</sup>

#### **2.2.4 Specifični izazovi u digitalizaciji bankarstva**

Jedan od ključnih izazova digitalizacije bankarstva je pravna neizvesnost koja proizlazi iz činjenice da postojeće zakonodavstvo često nije u koraku sa brzim tehnološkim promenama. Na primer, u Srbiji, Zakon o sprečavanju pranja novca i finansiranju terorizma zahteva fizičku identifikaciju klijenata prilikom otvaranja računa, što otežava potpunu digitalizaciju procesa. Takvi zahtevi su u suprotnosti sa trendovima u naprednim ekonomijama, gde je elektronska identifikacija (engl. e-KYC) omogućila bržu i efikasniju verifikaciju identiteta. Primera radi, Evropska unija je uvela eIDAS regulativu koja omogućava bezbednu elektronsku identifikaciju i potpisivanje ugovora na daljinu. Nedostatak ovakvih propisa u Srbiji usporava implementaciju digitalnih tehnologija i zahteva usklađivanje domaćeg zakonodavstva sa evropskim standardima.

---

<sup>20</sup> [https://www.ecb.europa.eu/euro/digital\\_euro/html/index.en.html](https://www.ecb.europa.eu/euro/digital_euro/html/index.en.html)

Prilagođavanje zakonskih okvira može omogućiti bankama u Srbiji da ponude potpuno digitalizovane usluge, smanje operativne troškove i povećaju konkurentnost na tržištu.<sup>21</sup>

Prema izveštaju Evropske agencije za sajber bezbednost (ENISA), broj sajber napada na finansijske institucije u Evropskoj uniji porastao je za 38% između 2020. i 2023. godine. Prosečan trošak po incidentu je 4,5 miliona evra i odnosi se na štetu pričinjenu finansijskim institucijama usled ovih napada. Glavni izazovi uključuju zaštitu podataka klijenata, otpornost sistema na hakerske napade i prevenciju finansijskih prevara. Moderne banke ulažu u biometrijsku autentifikaciju, višefaktorsku verifikaciju i napredne algoritme za detekciju prevara. Na primer, OTP banka u Srbiji koristi AI sisteme za praćenje transakcija u realnom vremenu, čime je smanjila pretnje prevara za 30%. Istovremeno, upotreba blokčejn tehnologije za zaštitu transakcija dodatno povećava sigurnost. Ipak, implementacija ovih rešenja zahteva značajne investicije, koje male i srednje banke mogu teško priuštiti, čime se dodatno povećava jaz između velikih banaka i manjih institucija. Ovi izazovi ukazuju na potrebu za regulatornim okvirom koji će osigurati jedinstvene standarde zaštite i kontinuirano testiranje otpornosti sistema.<sup>22</sup>

Razvoj digitalnih tehnologija kao što su distribuirane glavne knjige (DLT) i digitalne valute postavlja izazov interoperabilnosti – sposobnosti različitih sistema da međusobno komuniciraju i funkcionišu bez problema. Prema izveštaju Evropskog parlamenta (2024), čak 60% institucija u Evropskoj uniji navelo je tehničku nekompatibilnost kao ključnu prepreku uvođenju digitalnih valuta, što ukazuje na značajne izazove u pogledu usklađivanja infrastrukture i tehnoloških standarda na nivou Unije. Ova prepreka dodatno je pojačana obavezom poštovanja Opšte uredbe o zaštiti podataka (GDPR), koja zahteva napredne mehanizme šifrovanja i sigurnog rukovanja ličnim podacima tokom digitalnih transakcija. Kao odgovor na ove izazove, Evropska centralna banka (ECB) i druge relevantne institucije ulažu napore u razvoj standardizovanih API protokola i interoperabilnih digitalnih mreža, što predstavlja osnovu za bezbednu, efikasnu i široko prihvaćenu integraciju digitalnih finansijskih sistema u budućnosti.<sup>23</sup>

---

<sup>21</sup> <https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation>

<sup>22</sup> <https://www.enisa.europa.eu/>

<sup>23</sup> <https://www.ecb.europa.eu/>

Sve veća upotreba veštačke inteligencije (AI) i analitike velikih podataka (engl. Big Data) u bankarskom sektoru otvara pitanja transparentnosti algoritama i odgovornosti u procesu odlučivanja. AI algoritmi se sve češće koriste za procenu kreditnog rizika, detekciju prevara i personalizaciju ponuda klijentima. Međutim, studija OECD-a iz 2020. godine pokazuje da čak 53% korisnika izražava zabrinutost zbog nedostatka transparentnosti u radu algoritama. Postoji rizik da AI modeli mogu nenamerno stvoriti pristrasne odluke koje diskriminišu određene grupe korisnika na osnovu pola, rase ili socijalno-ekonomskog statusa. Da bi se to predupredilo, EU je donela Akt o veštačkoj inteligenciji (engl. AI Act), koji zahteva da algoritmi budu transparentni, proverljivi i usklađeni sa etičkim standardima. Banke u Srbiji suočavaju se sa izazovima u implementaciji ovih zahteva, jer je lokalno zakonodavstvo još uvek u procesu prilagođavanja evropskim standardima. Transparentnost i odgovornost algoritama ključni su za održavanje poverenja korisnika i regulatora u digitalne finansijske usluge.<sup>24</sup>

Evropska unija je prepoznala potrebu za balansiranjem između podsticanja inovacija i kontrole rizika u razvoju digitalnih tehnologija, te je uvela koncept regulatornih *sandbox* okruženja. Ova platforma omogućava testiranje novih tehnologija u kontrolisanim uslovima pre nego što budu u potpunosti odobrene za upotrebu na tržištu. Na primer, EU *Blockchain Sandbox*, pokrenut u februaru 2023. godine, omogućava testiranje blokčejn rešenja u sektorima finansija i osiguranja, sa ciljem smanjenja regulatornih neizvesnosti. Prema podacima Evropske komisije, preko 20 projekata godišnje ulazi u *sandbox* okruženja, omogućavajući regulatorima da unapred procene potencijalne rizike i benefite novih proizvoda. Srbija još uvek razvija slične inicijative, ali nedostatak ovih okruženja može usporiti usvajanje inovacija u bankarskom sektoru. Regulatorna *sandbox* platforma predstavlja kontrolisano okruženje koje omogućava bankama i *fintech* kompanijama da testiraju inovativna rešenja pod nadzorom regulatora, bez izlaganja širem finansijskom sistemu potencijalnim rizicima. Na taj način omogućava se razvoj i eksperimentisanje sa novim tehnologijama, dok se istovremeno obezbeđuje poštovanje regulatornih standarda i očuvanje sistemske stabilnosti. Ovakav pristup podstiče tehnološki napredak, a da pri tom ne narušava poverenje u finansijske institucije.<sup>25</sup>

---

<sup>24</sup> <https://www.europarl.europa.eu/>

<sup>25</sup> <https://digital-finance-platform.ec.europa.eu/>

## 2.2.5 Primeri regulatornih pristupa

### A. EU Digitalna strategija (2020)

Evropska unija je 2020. godine usvojila Digitalnu strategiju za finansijski sektor, postavljajući temelje za regulisanje i podsticanje digitalnih inovacija, uz istovremeno rešavanje izazova koje donosi digitalna transformacija.<sup>26</sup> Strategija se oslanja na četiri ključna prioriteta: smanjenje fragmentacije tržišta, olakšavanje digitalnih inovacija, stvaranje finansijskih podataka dostupnih korisnicima i rešavanje novih izazova digitalizacije. Cilj strategije je da obezbedi ravnotežu između inovacija i stabilnosti, povećavajući sigurnost i inkluzivnost u finansijskim uslugama (Milosevic et al., 2021).

Fragmentacija finansijskih tržišta unutar EU predstavljala je ključnu prepreku u razvoju integrisanog digitalnog finansijskog prostora. Strategija se fokusira na stvaranje jedinstvenog tržišta putem harmonizacije propisa i standarda kako bi se olakšalo pružanje prekograničnih digitalnih usluga. Inicijative poput SEPA<sup>27</sup> (engl. Single Euro Payments Area) omogućile su efikasnije plaćanje u evrima širom EU, dok su regulative poput PSD2<sup>28</sup> (engl. Payment Services Directive 2) stvorile osnove za Open Banking, povećavajući konkurenciju i inovacije (Mandic et al., 2014). Statistički podaci pokazuju da je do 2023. godine broj digitalnih transakcija unutar EU porastao za 35%, a broj korisnika digitalnih bankarskih usluga dostigao 60% odraslog stanovništva (Murinde et al., 2022). Ovaj rast ukazuje na značajan pomak ka digitalizaciji uz istovremeno smanjenje tržišnih barijera, čime se podstiče finansijska inkluzija.

Jedan od centralnih ciljeva strategije bio je podsticanje razvoja novih tehnologija poput veštačke inteligencije (AI), blokčejna i analitike velikih podataka u finansijskom sektoru. EU je uvela pravni okvir koji omogućava kompanijama da testiraju svoje proizvode kroz regulatorne *sandbox* modele, slične onima u Velikoj Britaniji, omogućavajući kontrolisano eksperimentisanje uz minimalne

---

<sup>26</sup> [https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age\\_en](https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en)

<sup>27</sup> SEPA omogućava građanima i kompanijama unutar Evropskog ekonomskog prostora (EEA) jednostavna i sigurna plaćanja u evrima, kao da se transakcije obavljaju unutar jedne zemlje. Ovaj sistem pojednostavljuje prekogranične transakcije i smanjuje troškove. Povezan je sa harmonizacijom finansijskih tržišta i smanjenjem fragmentacije u okviru EU digitalne strategije.

<sup>28</sup> PSD2 je direktiva EU koja promovise razvoj Open Banking sistema. Omogućava trećim stranama da koriste podatke klijenata za pružanje inovativnih finansijskih usluga, uz obaveznu saglasnost korisnika. Cilj je povećanje konkurencije i transparentnosti. Ključna za razvoj digitalnih plaćanja i implementaciju novih tehnologija, što je u skladu sa istraživanjem o digitalnim inovacijama.

regulatorne prepreke (Khuong et al., 2022). Uvođenjem *Digital Operational Resilience Act* (DORA) EU je osnažila zaštitu informacionih sistema i podataka korisnika, čime je povećala poverenje u digitalne tehnologije. Prema izveštaju Evropske komisije iz 2023. godine, ulaganja u *fintech* sektor u EU porasla su za 47%, dok je upotreba blokčejn tehnologije u bankarstvu povećana za 29% u odnosu na prethodnu godinu (Milosevic et al., 2021).

Digitalna strategija EU naglašava važnost pristupa podacima kako bi se omogućila bolja personalizacija usluga i konkurencija među pružaocima finansijskih usluga. *Open Finance* inicijativa, koja je proširenje direktive PSD2, osigurava korisnicima pravo na upravljanje svojim finansijskim podacima i deljenje istih sa trećim stranama uz njihovu saglasnost. Ovo je omogućilo razvoj inovativnih rešenja kao što su platforme za lične finansije i automatizovane investicione aplikacije. Prema istraživanju (Milošević et al., 2018), digitalizacija podataka u finansijama omogućila je smanjenje troškova upravljanja kreditima za 30% i povećanje tačnosti procene kreditnog rizika za 25%.

Digitalna strategija prepoznaje izazove kao što su sajber bezbednost, transparentnost algoritama i zaštita privatnosti, koji prate brz razvoj digitalnih tehnologija. Uvođenjem MiCA regulative, EU je postavila pravila za regulisanje tržišta krypto-imovine, uključujući *stablecoins*, čime se smanjuju rizici od pranja novca i finansiranja terorizma (Murinde et al., 2022). Dodatno, već pomenuta DORA regulativa nalaže finansijskim institucijama stroge standarde otpornosti na sajber napade i operativne rizike, uključujući obavezno testiranje i identifikaciju ranjivosti sistema (Milosevic et al., 2021). Statistički podaci ukazuju da je uvođenjem ovih regulativa smanjen broj sajber napada na bankarski sektor EU za 15% u 2022. godini, dok je nivo poverenja korisnika u digitalne usluge porastao za 18% (Mandic et al., 2014).

EU Digitalna strategija iz 2020. godine predstavlja sveobuhvatan okvir za regulaciju i razvoj digitalnih finansijskih usluga, balansirajući između inovacija i bezbednosti. Postignuti rezultati, kao što su povećana upotreba digitalnih platformi, rast investicija u *fintech* sektor i smanjenje sajber rizika, ukazuju na uspešnost ovog pristupa (Milosevic et al., 2021; Murinde et al., 2022). Primena ovih principa u Srbiji mogla bi značajno unaprediti finansijski sektor, omogućavajući mu da odgovori na savremene izazove i postane konkurentniji na globalnom nivou. Uvođenje Open

Banking inicijativa, *sandbox* modela i alata za zaštitu podataka ključno je za stvaranje otpornog i inovativnog digitalnog ekosistema.

## B. Azijski modeli regulacije

Azijske zemlje, poput Singapura i Malezije, razvile su napredne regulatorne okvire za digitalno bankarstvo, koji su omogućili lakši ulazak novih igrača na tržište, povećali konkurenciju i podstakli finansijsku inkluziju, naročito među malim i srednjim preduzećima i pojedincima sa ograničenim pristupom tradicionalnim finansijskim uslugama. Njihov pristup zasnovan je na fleksibilnosti i strogo definisanim standardima bezbednosti, kao i na podsticanju inovacija, čime je stvoren regulatorni okvir koji odgovara potrebama savremenog bankarskog tržišta.<sup>29</sup>

Slično tome, rad (Doran et al., 2022) ukazuje da je pandemija COVID-19 dodatno ubrzala digitalizaciju finansijskog sektora u Srednjoj i Istočnoj Evropi, naglašavajući značaj tehnoloških inovacija za održavanje efikasnosti i stabilnosti sistema u izazovnim okolnostima.

Singapur je primer zemlje sa jednim od najnaprednijih regulatornih sistema za digitalne banke koji je 2019. godine omogućio izdavanje dve vrste licenci: Digitalne pune banke (DFB), koje pružaju širok spektar usluga pojedincima i MSP-ima, i Digitalne banke sa ograničenim licencama (DWB), fokusirane na poslovanje sa MSP-ima. Ove licence prate stroge zahteve u pogledu kapitalne adekvatnosti, gde je početni kapital za DFB postavljen na 15 miliona SGD, uz postepeno povećanje na 1,5 milijardi SGD. Singapurski regulator, Monetarna uprava Singapura (MAS), uveo je i fazni pristup razvoju, koji omogućava postepeno širenje poslovanja nakon uspešnog testiranja osnovnih operacija. Pored toga, digitalne banke u Singapuru moraju ispuniti visoke standarde u vezi sa sajber bezbednošću, uključujući biometrijsku autentifikaciju<sup>30</sup> i višefaktorsku verifikaciju, kao i usklađenost sa Zakonom o zaštiti podataka. Prema MAS-u, do kraja 2023. godine, digitalne banke privukle su više od 500.000 korisnika i odobrile kredite vredne 1,2 milijarde SGD, čime su značajno povećale pristup finansijskim uslugama. Ovi rezultati potvrđuju istraživanje (Häggqvista, 2019) o digitalnoj transformaciji u švedskom bankarskom sektoru, koje naglašava važnost tehnoloških inovacija za povećanje efikasnosti i dostupnosti usluga.

---

<sup>29</sup> <https://www.mckinsey.com/>

<sup>30</sup> Ove tehnologije omogućavaju analizu velikih podataka u realnom vremenu, smanjujući lažno pozitivne rezultate i ubrzavajući vreme reagovanja.

S druge strane, Malezija je implementirala sličan, ali specifično prilagođen model, fokusiran na podsticanje konkurencije i povećanje finansijske inkluzije. Centralna banka Malezije (engl. Bank Negara Malaysia) uvela je regulativu za digitalne banke 2020. godine, omogućavajući izdavanje posebnih licenci namenjenih pružanju usluga populaciji sa ograničenim pristupom finansijama. Početni kapital za banke u Maleziji postavljen je na 100 miliona RM, uz obavezu povećanja na 300 miliona RM tokom pet godina, dok su banke prošle kroz fazu razvoja od tri do pet godina kako bi se osigurala usklađenost sa propisima i stabilnost poslovanja. Kao deo strategije, Malezija je zahtevala da banke usmere svoje usluge ka MSP-ima, startapima i ruralnim područjima, čime su povećale pristupačnost finansijskih usluga za 20% u tim segmentima. Statistički podaci pokazuju da su prve digitalne banke u Maleziji obradile više od 1 milion transakcija u prvoj godini i odobrile kredite vredne 850 miliona RM, pri čemu je 65% sredstava bilo usmereno ka MSP-ima. Ovi rezultati potvrđuju zaključke rada (Hodula, 2022) o ulozi finteka kao zamene za tradicionalne kreditne institucije u globalnom finansijskom sistemu, posebno u zemljama u razvoju.

Iako modeli Singapura i Malezije dele mnoge zajedničke karakteristike, poput postepenog licenciranja, stroge kontrole rizika i fokusiranosti na finansijsku inkluziju, postoji razlika u prioritetima. Dok je Singapur naglasak stavio na tehnološki napredne servise i globalne kompanije poput Grab i Sea Group, Malezija se fokusirala na lokalne potrebe i razvoj startapa i MSP-ova. Statistički podaci potvrđuju uspeh oba pristupa – Singapur je zabeležio 1,5 miliona novih korisnika i obradio digitalne transakcije u vrednosti od 3,2 milijarde SGD, dok je Malezija povećala pristup finansijama za 20% u ruralnim područjima i usmerila 65% kredita ka MSP-ima. Ovi modeli pružaju smernice za druge zemlje, uključujući Srbiju, koje teže modernizaciji svojih finansijskih sistema. Njihovo iskustvo pokazuje kako regulatorni pristup koji kombinuje inovacije i sigurnost može stvoriti efikasnije i konkurentnije tržište, što je ključno za ubrzanje digitalizacije u bankarstvu.<sup>31</sup>

### C. *Sandbox* modeli u Velikoj Britaniji

Velika Britanija je postavila standard u razvoju regulatornih *sandbox* modela, omogućavajući kompanijama da testiraju inovativne finansijske proizvode i usluge u kontrolisanom okruženju. Financial Conduct Authority (FCA), regulatorno telo Velike Britanije, 2016. godine lansiralo je

---

<sup>31</sup> <https://www.mckinsey.com/>

prvi regulatorni *sandbox* program, koji je kasnije prepoznat kao globalni model za podršku *fintech* inovacijama i bezbednoj implementaciji digitalnih rešenja. Ovaj pristup je posebno značajan za povećanje finansijske stabilnosti i omogućavanje bržeg prihvatanja novih tehnologija u bankarstvu, kao što su veštačka inteligencija (AI), blokčejn i automatizovani procesi (Milosevic et al., 2021).

Prema FCA-u, regulatorni *sandbox* obuhvata četiri ključna elementa:

- Ograničeno tržišno testiranje – Kompanijama se omogućava testiranje proizvoda u stvarnim uslovima sa kontrolisanim rizicima, što omogućava efikasniju procenu tržišnog potencijala i bezbednosnih aspekata.
- Pravna fleksibilnost – Privremena regulatorna izuzeća omogućavaju testiranje proizvoda bez potpunog regulatornog odobrenja, uz postepeno prilagođavanje zakonodavstvu.
- Savetodavna podrška – FCA pruža stručno vođenje, čime pomaže učesnicima da zadovolje zahteve usklađenosti i povećaju bezbednost operacija.
- Zaštita potrošača – *Sandbox* modeli uključuju stroge mere zaštite korisnika, minimizirajući potencijalne rizike zloupotrebe i povećavajući transparentnost finansijskih proizvoda.

Ove karakteristike su omogućile značajan napredak u testiranju i implementaciji novih tehnologija, što je potvrđeno istraživanjem (Milošević et al., 2018), koje ističe da digitalna ekonomija u Evropi zahteva fleksibilne regulatorne okvire kako bi se obezbedila stabilnost uz inovativnost.

Prema FCA izveštaju, do kraja 2021. godine, više od 137 kompanija prošlo je kroz *sandbox* programe, pri čemu je preko 80% njih uspešno nastavilo poslovanje nakon testiranja. Ovi programi omogućili su firmama smanjenje troškova implementacije i do 40%, dok su investicije u *fintech* sektor porasle za 36% u periodu od 2016. do 2021. godine (Murinde et al., 2022).

*Fintech* kompanije, poput Revolut i Starling Bank, koristile su *sandbox* modele za testiranje mobilnog bankarstva i biometrijske autentifikacije, čime su značajno unapredile korisničko iskustvo i bezbednost transakcija. Ove tehnologije su dodatno potvrdile efikasnost *sandbox* okruženja u razvoju inovativnih rešenja, što su istraživanja (Khuong et al., 2022) potvrdila kao ključne faktore prihvatanja digitalnog bankarstva u zemljama poput Vijetnama.

Srbija, prema analizi finansijskih parametara banaka koje su sproveli (Mandic et al., 2014), još uvek pokazuje visok nivo oslanjanja na tradicionalne metode procene rizika i pružanja usluga. Međutim, rezultati ove analize ukazuju na potrebu za primenom inovativnih pristupa kako bi se povećala efikasnost poslovanja i smanjili operativni troškovi.

Korišćenjem *sandbox* modela, srpske banke mogle bi značajno smanjiti vreme potrebno za testiranje novih proizvoda, omogućavajući im da brzo reaguju na promene tržišta i povećaju konkurentnost. Pored toga, u radu (Milosevic et al., 2021) se ističe da integracija digitalnih tehnologija, uključujući AI analitiku i blokčejn, može poboljšati procese donošenja odluka i predikciju rizika, čime se smanjuju troškovi obrade transakcija i povećava sigurnost sistema.

Uvođenje *sandbox* modela u Srbiji omogućilo bi lakšu implementaciju digitalnih novčanih platformi i automatizovanih sistema za upravljanje podacima, posebno u kontekstu Open Banking inicijativa. Ovo je važno jer bi, prema studiji (Murinde et al., 2022), *sandbox* modeli mogli smanjiti regulatorne prepreke i podstaći inovacije, povećavajući finansijsku inkluziju i stabilnost sektora.

Regulatorni *sandbox* modeli u Velikoj Britaniji pokazali su se kao ključni instrumenti za ubrzavanje inovacija i testiranje novih finansijskih tehnologija u sigurnom i kontrolisanom okruženju. Njihova primena omogućila je brži rast *fintech* sektora, smanjenje regulatornih prepreka i povećanje sigurnosti korisnika, što je potvrđeno istraživanjima (Mandic et al., 2014) i (Milosevic et al., 2021). Primena ovih modela u Srbiji mogla bi doprineti unapređenju digitalnog bankarstva, smanjenju troškova operacija i povećanju finansijske inkluzije, čime bi se domaći bankarski sektor pripremio za buduće izazove. Razvoj *sandbox* okruženja omogućio bi brže testiranje tehnologija poput veštačke inteligencije, blokčejna i biometrijske autentifikacije, pružajući srpskim bankama konkurentsku prednost na globalnom tržištu.

## **2.3 Izazovi u onlajn plaćanjima i elektronskom načinu plaćanja**

Onlajn plaćanja postala su ključni deo savremenog finansijskog sistema, omogućavajući korisnicima brz i efikasan prenos novca. Prema istraživanju, očekuje se da vrednost digitalnih transakcija dostigne 14,78 biliona dolara do 2027. godine, dok se globalni trošak sajber kriminala procenjuje na 9,5 biliona dolara do 2024. godine. Ove brojke jasno ukazuju na potrebu za

unapređenjem bezbednosnih sistema i implementacijom modernih tehnologija radi zaštite korisnika i poslovnih subjekata (Demkovych, 2023).

### **2.3.1 Onlajn plaćanja i bezbednosni izazovi u digitalnim transakcijama**

Proces digitalnih plaćanja uključuje različite metode, kao što su bankarske kartice, internet bankarstvo, SMS plaćanja i elektronski novčanici. Sve transakcije funkcionišu putem sistema kao što su Visa, MasterCard ili PayPal, gde korisnik unosi podatke i pokreće prenos sredstava. Najveći izazov predstavlja osiguranje da nalog za plaćanje zaista potiče od vlasnika računa, a ne od prevaranta (Revathi, 2019). Kada se koriste bankarske kartice, PIN kodovi i CVC/CVV brojevi deluju kao lozinke poznate samo vlasnicima računa. Nasuprot tome, sistemi daljinskog bankarstva pružaju dodatne slojeve zaštite, uključujući jednokratne lozinke i elektronske potpise. Elektronski novčanici omogućavaju veću fleksibilnost, ali često nemaju istu regulatornu zaštitu kao tradicionalni bankovni računi (Khuong et al., 2022).

Porast digitalnih transakcija prati povećanje rizika od sajber kriminala. Među ključnim problemima izdvajaju se sigurnost ličnih podataka, sajber napadi na onlajn prodavnice, lažne 3-D Secure stranice, „blizanci“ bankarskih sajtova i lažni zahtevi za provizijama. Sigurnost ličnih podataka često je ugrožena zbog neusklađenosti kompanija sa regulativama, dok DDoS napadi na onlajn prodavnice postaju sve učestaliji. Rešenja uključuju DLP sisteme i redovne bezbednosne provere (PWC, 2016). Prevaranti koriste sofisticirane metode, poput kopiranja 3-D Secure stranica i bankarskih sajtova, kako bi prikupili poverljive podatke korisnika, naglašavajući potrebu za boljom edukacijom i implementacijom tehnologija kao što su 3DS 2.0 i SSL sertifikati (Revathi, 2019; OECD, 2020).

Zaštita podataka u onlajn transakcijama može se unaprediti primenom sigurnih metoda plaćanja. PayPal pruža visoku sigurnost povezivanjem sa međunarodnim bankarskim karticama, dok Visa i MasterCard nude dodatnu zaštitu putem virtuelnih kartica. Elektronski novčanici smanjuju rizik jer ne zahtevaju unos osetljivih podataka tokom transakcija, dok kripto novčanici koriste privatne ključeve i šifrovane protokole za sigurnost virtuelnih sredstava (Khuong et al., 2022). Implementacijom ovih metoda, korisnici mogu dodatno zaštititi svoje finansije u digitalnom okruženju.

S obzirom na rastuće pretnje, finansijske institucije primenjuju različite strategije za zaštitu. Dvofaktorska autentifikacija (2FA) pruža dodatni sloj sigurnosti kombinovanjem lozinke i jednokratnog koda, dok tokenizacija podataka omogućava zaštitu kroz pretvaranje podataka u tokene koji se mogu analizirati bez izlaganja stvarnih informacija (PWC, 2016). Osim toga, SSL sertifikati osiguravaju enkriptovanu komunikaciju između korisnika i servera, a biometrijske verifikacije, uključujući prepoznavanje lica i otisaka prstiju, pružaju sigurnu proveru identiteta bez fizičkog prisustva (Demkovich, 2023). Ove mere značajno smanjuju mogućnosti prevarnih aktivnosti.

Preduzeća dodatno unapređuju sigurnost primenom sledećih mera: praćenje transakcija u realnom vremenu omogućava brzo prepoznavanje i blokiranje prevarnih aktivnosti, dok edukacija zaposlenih i klijenata o metodama socijalnog inženjeringa i fišing napadima smanjuje rizike (Pavithra & Geetha, 2021). Implementacija AI algoritama omogućava automatizovano prepoznavanje prevara, dok ograničavanje nepotrebnih opcija plaćanja smanjuje ulazne tačke za napadače (Murinde et al., 2022). Ovaj sveobuhvatni pristup omogućava bankama i preduzećima da unaprede svoje sisteme zaštite, povećavajući poverenje korisnika u digitalne finansijske usluge.

### **2.3.2 Prepoznavanje izazova kod elektronskih plaćanja**

Elektronska plaćanja postala su ključni deo savremenih finansijskih sistema, omogućavajući brze i sigurne transakcije u okviru globalne e-trgovine. Prema podacima Svetskog ekonomskog foruma (2018), elektronska plaćanja omogućavaju malim i srednjim preduzećima lakši pristup međunarodnim tržištima, čime se smanjuju troškovi poslovanja i povećava dostupnost proizvoda i usluga. Uprkos očiglednim prednostima, ovaj sektor se suočava sa nizom izazova, uključujući regulatorne barijere, sigurnosne rizike i tehnička ograničenja koja mogu ometati njegov dalji razvoj.

Sistem elektronskih plaćanja obuhvata širok spektar učesnika, uključujući krajnje korisnike (kupce i preduzeća), provajdere usluga plaćanja (PSP) i međunarodne mreže poput Visa, MasterCard i PayPal. Uspostavljanje efikasnih mehanizama za saradnju između ovih učesnika od suštinskog je značaja za osiguranje interoperabilnosti i stabilnosti sistema. Moderna plaćanja, kao što su mobilna plaćanja i elektronski novčanici, dodatno unapređuju dostupnost finansijskih usluga, naročito u zemljama u razvoju, gde veliki deo populacije nema pristup tradicionalnim bankarskim uslugama.

Međutim, rast e-trgovine prate i bezbednosni izazovi. Prema podacima Deutsche Bank Research (2020), sajber kriminal i prevare postaju sve češći, zbog čega je potrebno jačanje bezbednosnih protokola kroz dvofaktorsku autentifikaciju, tokenizaciju podataka i korišćenje SSL sertifikata za zaštitu transakcija, kao i kontinuirano ulaganje u nove tehnologije, poput veštačke inteligencije (AI) i blokčejna, kako bi obezbedili pouzdane i sigurne transakcije.

Regulatorni okvir takođe igra ključnu ulogu u daljem razvoju e-plaćanja. Prema preporukama (Davies, 2020), regulatorne politike moraju biti prilagođene tehnološkim inovacijama, omogućavajući istovremeno zaštitu korisnika i podsticanje konkurencije. Uključivanje tzv. *sandbox* okvira za testiranje novih tehnologija može ubrzati inovacije u sektoru i istovremeno smanjiti rizike povezane sa digitalnim transakcijama.

Ipak, ograničenja u prekograničnim transakcijama i različiti nacionalni propisi predstavljaju značajne prepreke. Studija (Fernández-Villaverde & Sanches, 2019) ističe da harmonizacija regulativa i standardizacija sistema plaćanja mogu olakšati međunarodnu trgovinu i smanjiti troškove konverzije valuta, što je posebno važno za zemlje u razvoju, gde nedostatak infrastrukture i regulatorne podrške često otežava pristup globalnim tržištima.

Jedno od ključnih rešenja jeste unapređenje infrastrukture plaćanja. Preporuke Svetske banke<sup>32</sup> uključuju uvođenje interoperabilnih sistema i digitalnih identifikacionih mehanizama koji omogućavaju proveru identiteta korisnika i olakšavaju pristup finansijskim uslugama. Integracija naprednih tehnologija, biometrijske autentifikacije i kriptovaluta, dodatno doprinosi sigurnosti i efikasnosti transakcija.

## **2.4 Sprečavanje prevara i zaštita podataka u digitalnim transakcijama**

Digitalizacija bankarskih usluga donela je značajnu efikasnost i dostupnost, ali je istovremeno otvorila vrata sofisticiranim prevarama koje ugrožavaju bezbednost klijenata i integritet finansijskih institucija. Prema izveštaju Federalne trgovinske komisije (FTC), u 2021. godini zabeleženo je 2,8 miliona prijavljenih slučajeva prevara, pri čemu su ukupni gubici iznosili 5,8 milijardi dolara. Štaviše, prema Američkom bankarskom žurnalu (American Banking Journal),

---

<sup>32</sup> <https://id4d.worldbank.org>

svaki izgubljeni dolar usled prevara košta banke dodatna četiri dolara zbog troškova saniranja štete, pravnih sporova i narušavanja reputacije. Kako bi odgovorile na ove izazove, banke sve više ulažu u napredne tehnologije za detekciju i prevenciju prevara, s ciljem jačanja poverenja korisnika i minimiziranja rizika (Murinde et al., 2022).

### **2.4.1 Uobičajeni primeri digitalnih prevara**

Digitalne prevare poprimaju različite oblike, uključujući fišing napade, krađu identiteta i lozinki, žičane prevare<sup>33</sup> i pranje novca. Fišing napadi ostaju najzastupljeniji, jer prevaranti koriste e-poštu, poruke i telefonske pozive kako bi prikupili lične podatke korisnika i instalirali zlonamerni softver. Prema istraživanjima OECD-a (2020), 96% korisnika banaka smatra zaštitu od prevara ključnim faktorom prilikom izbora banke. Osim toga, sofisticirane metode poput biometrijskih prevara, gde prevaranti koriste ukradene otiske prstiju i slike, dodatno komplikuju borbu protiv kriminala. Ove nove pretnje zahtevaju uvođenje višefaktorskih autentifikacija, veštačke inteligencije (AI) i analitike velikih podataka za prepoznavanje sumnjivih obrazaca ponašanja u realnom vremenu (Khuong et al., 2022).

### **2.4.2 Otkrivanje i sprečavanje bankarskih prevara**

Otkrivanje i sprečavanje bankarskih prevara obuhvata skup strategija, politika i tehnologija usmerenih na zaštitu finansijskih institucija, njihovih sistema i klijenata od prevarnih aktivnosti. Proces otkrivanja zasniva se na praćenju pretnji u realnom vremenu, analiziranju ponašanja korisnika i proaktivnoj identifikaciji rizika, dok se prevencija fokusira na ublažavanje rizika kroz interne kontrole, obuke zaposlenih i višeslojne sisteme zaštite. Savremena rešenja oslanjaju se na veštačku inteligenciju (AI) i mašinsko učenje (ML), koji analiziraju ogromne količine transakcijskih podataka radi otkrivanja nepravilnosti i obrazaca prevara u realnom vremenu, omogućavajući brzo prilagođavanje novim pretnjama. Pored toga, biometrijska autentifikacija, uključujući otisak prsta i prepoznavanje lica, pruža dodatnu sigurnost jer koristi jedinstvene fizičke karakteristike korisnika koje je teško falsifikovati. U kombinaciji sa dvofaktorskom (2FA) i multifaktorskom autentifikacijom (MFA), kao i naprednim analitikama, ove tehnologije omogućavaju predviđanje prevarnog ponašanja, smanjenje lažno pozitivnih rezultata i poboljšanje

---

<sup>33</sup> Wire fraud – oblik finansijske prevare u kojoj se elektronskim putem (bankovni transferi, SWIFT uplate) nezakonito prisvaja novac, često korišćenjem lažnih naloga, falsifikovanih instrukcija za plaćanje ili hakovanih računa.

vremena reagovanja. Integracijom ovih inovacija, finansijske institucije mogu proaktivno zaštititi svoje resurse i poverenje klijenata u sve digitalizovanijem okruženju.

### **2.4.3 Strategije za borbu protiv prevara u bankarstvu**

Prevenција i otkrivanje prevara u bankarskom sektoru zahteva sveobuhvatan pristup koji kombinuje tehnološka rešenja, interne kontrole i edukaciju. Prema (Pavithra & Geetha, 2021), ključni faktori za percepciju korisnika prema digitalnim bankarskim uslugama uključuju sigurnost i poverenje, što dodatno naglašava potrebu za višeslojnim pristupom u zaštiti sistema. Jedna od osnovnih strategija je organizovanje redovnih obuka o prevarama za zaposlene, jer su oni često mete sajber-napada, posebno fišinga i socijalnog inženjeringa. Edukacija osoblja o prepoznavanju potencijalnih pretnji i pravilnim postupcima u slučaju sumnje na prevaru značajno smanjuje rizike. Pored toga, pažnja treba biti usmerena na internu prevaru, jer zaposlenima koji imaju pristup osetljivim podacima može biti pružena prilika za zloupotrebu položaja. Preporučuje se praćenje aktivnosti zaposlenih, kao što su neuobičajene transakcije, prekomerni prenos sredstava i vanredno radno vreme (PWC, 2016). Izgradnja baze podataka o pretnjama omogućava institucijama da prate nove pretnje i pravovremeno reaguju. Kombinovanjem unutrašnjih i spoljašnjih podataka, banke mogu razviti sveobuhvatan pregled rizika i obučavati osoblje na osnovu konkretnih primera. Takođe, edukacija klijenata je podjednako važna, jer informisani korisnici postaju prvi nivo odbrane protiv prevara. Kampanje za podizanje svesti o bezbednosnim merama, poput dvofaktorske autentifikacije (2FA) i biometrijske zaštite, povećavaju verovatnoću da će korisnici koristiti ove opcije (Revathi, 2019). Praćenje transakcija u realnom vremenu ključno je za otkrivanje anomalija u obrascima ponašanja klijenata, omogućavajući brzo reagovanje na sumnjive aktivnosti. Razvijanjem profilnih obrazaca ponašanja, banke mogu efikasno razlikovati legitimne transakcije od prevarnih pokušaja. Konačno, razvijanje višeslojnih sigurnosnih sistema podrazumeva kombinovanje administrativnih, fizičkih i tehničkih mera zaštite. Administrativne mere uključuju politike lozinki i programe obuke, dok fizičke mere obuhvataju ograničen pristup podacima i redovne provere kontrolnih zapisa. Tehničke mere, poput zaštitnih zidova, antivirusnih programa i sistema za praćenje prevara zasnovanih na veštačkoj inteligenciji, dodatno smanjuju ranjivosti sistema. Implementacijom ovih strategija, banke mogu znatno smanjiti rizike i ojačati poverenje klijenata u digitalne finansijske usluge.

#### 2.4.4 Napadi socijalnog inženjeringa i mere zaštite

Napadi socijalnog inženjeringa predstavljaju jednu od najsofisticiranijih pretnji u digitalnom okruženju, posebno u kontekstu upotrebe kriptovaluta i elektronskog bankarstva. Ove vrste napada oslanjaju se na manipulaciju ljudima, a ne na tehničke ranjivosti, kako bi prevarom došli do poverljivih informacija kao što su lozinke, privatni ključevi, brojevi računa i finansijski podaci. Napadači koriste psihološke tehnike zasnovane na poverenju, autoritetu ili strahu, čime žrtve dovode u situaciju da nenamerno otkriju ključne informacije ili obave štetne radnje. Razvoj digitalnih platformi i rast popularnosti kriptovaluta stvorili su nove prilike za ovakve pretnje, čime je njihovo istraživanje i razumevanje postalo ključno za zaštitu korisnika (Stankić et al., 2023).

Napadi socijalnog inženjeringa mogu se podeliti u tri osnovne kategorije: tehnološki, ljudski i hibridni napadi. Tehnološki napadi koriste softverske alate i aplikacije kako bi prevarili korisnike da preuzmu zlonamerni softver ili podele svoje poverljive informacije. Neke od najčešćih tehnoloških pretnji uključuju špijunski softver (engl. spyware), koji diskretno prikuplja informacije o korisnicima, *adware* koji prikazuje neželjene reklame, *keyloggere* koji beleže unete lozinke, *ransomware* koji blokira pristup podacima dok se ne plati otkup, trojance koji omogućavaju napadačima pristup uređajima, kao i računarske crve koji mogu uništiti podatke ili usporiti rad sistema (Šimberová & Kita, 2020). Ove vrste napada često koriste sigurnosne propuste i nedostatak ažuriranog softvera kako bi ostvarile pristup sistemima.

Ljudski napadi oslanjaju se na direktnu manipulaciju korisnicima. Najčešći oblici ovih napada uključuju lažno predstavljanje, gde se napadači pretvaraju da su legitimne osobe (npr. IT podrška) kako bi prevarili korisnike da otkriju poverljive informacije. Pristupi kao što su *tailgating*, gde napadač fizički prati ovlašćenog korisnika u sigurni prostor, prisluškivanje telefonskih razgovora, posmatranje lozinki preko ramena (engl. shoulder surfing) i prevara putem lažnih scenarija (engl. pretexting) posebno su opasni u digitalnim i fizičkim okruženjima. Ove tehnike koriste ljudsku radoznalost, poverenje i želju da pomognu, čineći ih efikasnim čak i protiv obazrivih korisnika (Vives, 2019).

Hibridni napadi kombinuju tehničke i ljudske metode, stvarajući višestruke slojeve obmane. Primeri uključuju *baiting*, gde napadači ostavljaju zaražene USB uređaje ili CD-ove na javnim mestima, nadajući se da će ih žrtve priključiti na svoje uređaje, *trolling*, koji koristi manipulaciju

javnim mišljenjem i emocionalne reakcije, fišing, koji putem imejlova preusmerava korisnike na lažne sajtove, i *pharming*, koji menja DNS postavke kako bi preusmerio korisnike na zlonamerne verzije legitimnih sajtova. *Smishing* napadi koriste SMS poruke sa zlonamernim linkovima, dok napadi tipa *whaling* ciljaju visoke rukovodioce koristeći personalizovane pretnje (Stankić, 2021). Ovi napadi, zbog svoje kombinovane prirode, često zaobilaze osnovne mere zaštite, čineći ih posebno opasnim.

Napadi socijalnog inženjeringa ozbiljno ugrožavaju sigurnost korisnika digitalnih valuta i elektronskog bankarstva. Kriptovalute, zahvaljujući svojoj pseudonimnosti, posebno su privlačne napadačima, jer omogućavaju anonimne transakcije koje je teško pratiti. Fišing napadi su među najčešće korišćenim tehnikama, uključujući složene strategije poput MITM (engl. *Man-in-the-Middle*) napada, gde hakeri presreću komunikaciju između banke i korisnika, krađući poverljive podatke. S obzirom na to da korisnici često nisu svesni napada, posledice mogu uključivati finansijske gubitke, krađu identiteta i ozbiljna narušavanja privatnosti (PWC, 2016).

Zaštita od ovih napada zahteva kombinaciju tehnoloških rešenja i edukacije korisnika. Mere zaštite uključuju dvofaktorsku autentifikaciju (2FA), redovno ažuriranje softvera i antivirusnih programa, svesnost o potencijalnim pretnjama, proveru autentičnosti imejlova i poruka, kao i simulacije fišing napada kako bi se proverila otpornost korisnika. Poseban naglasak stavlja se na zaštitu ličnih podataka i šifrovanu komunikaciju, čime se dodatno smanjuje rizik od neovlašćenog pristupa. Uvođenje sigurnosnih politika i protokola, kao i postavljanje jasnih pravila za upravljanje lozinkama i privatnim ključevima, od suštinskog je značaja za sprečavanje napada (Revathi, 2019).

### **3 UTICAJ DIGITALNIH TEHNOLOGIJA NA BANKARSKI SEKTOR U SRBIJI**

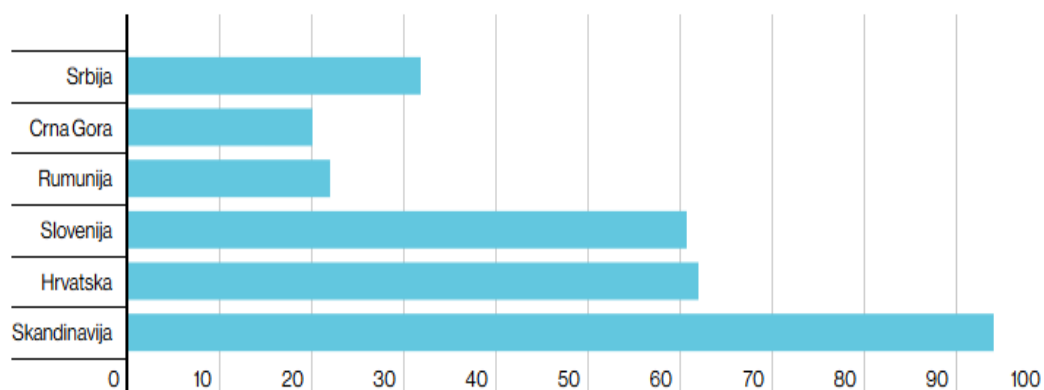
Digitalizacija bankarskog sektora predstavlja temelj savremenog finansijskog sistema, jer omogućava bržu, sigurniju i dostupniju uslugu za klijente, istovremeno unapređujući konkurentnost i otpornost banaka. U kontekstu Srbije, ovaj proces postaje sve izraženiji — banke ubrzano implementiraju digitalne proizvode i usluge kako bi povećale profitabilnost, unapredile korisničko iskustvo i poboljšale operativnu efikasnost. Trenutno stanje digitalizacije u Srbiji pokazuje stalni napredak, uz fokus na unapređenje sigurnosti, veću automatizaciju i podizanje kvaliteta usluga kroz primenu savremenih digitalnih rešenja.

#### **3.1 Analiza trenutnog stanja digitalizacije**

Digitalna transformacija bankarstva uključuje optimizaciju poslovnih procesa, uvođenje automatizovanih sistema, modernizaciju infrastrukture i unapređenje bezbednosti transakcija (Maksic, Golitsis, Radev, & Gkasis, 2024).

Analiza pokazuje da gotovo sve banke u Srbiji nude osnovne digitalne usluge. Od ukupno 31 banke, 29 pruža internet bankarstvo, 24 nudi mobilno bankarstvo, dok 30 koristi SMS servise za informisanje klijenata. Pored toga, banke su razvile mobilne aplikacije koje omogućavaju beskontaktna plaćanja, podizanje gotovine putem mobilnih telefona, skeniranje čekova i upravljanje računima u realnom vremenu (Maksic et al., 2024; Stankić et al., 2023).

U poređenju sa državama regiona i razvijenim evropskim zemljama, digitalizacija bankarskih usluga u Srbiji se nalazi na srednjem nivou. Kao što prikazuje Slika 5, udeo korisnika digitalnog bankarstva u Srbiji je značajno viši nego u Crnoj Gori i Rumuniji, ali i dalje zaostaje za Slovenijom, Hrvatskom, a naročito za skandinavskim zemljama, gde taj procenat gotovo dostiže 100%. Ovi podaci dodatno potvrđuju potrebu za intenzivnijim razvojem digitalnih platformi i povećanjem digitalne inkluzije u Srbiji.



Slika 4. Procenat populacije koja koristi digitalne bankarske usluge u Srbiji u odnosu na odabrane zemlje<sup>34</sup>

Mobilno bankarstvo postaje dominantan kanal za digitalne usluge, sa konstantnim rastom broja korisnika u prethodnoj deceniji. U periodu između 2013. i 2016. godine, broj korisnika mobilnog bankarstva u Srbiji povećao se za 649.030, dok je broj korisnika internet bankarstva porastao za 626.933. Ovaj trend ukazuje na rastuću potrebu za brzim, dostupnim i fleksibilnim finansijskim rešenjima, čime mobilne aplikacije i digitalni servisi postaju ključni alat u strategijama banaka (Maksic et al., 2024).

Banke u Srbiji ulažu u razvoj multifunkcionalnih bankomata koji omogućavaju uplate, podizanje gotovine i plaćanje računa. Ovi uređaji značajno smanjuju potrebu za fizičkom posetom filijalama, čime se ubrzava proces transakcija i povećava operativna efikasnost. ProCredit banka je prva uvela samouslužne zone koje omogućavaju 24/7 usluge, čime se klijentima pruža dodatna fleksibilnost.

Iako digitalizacija bankarskog sektora ubrzano napreduje, postoje regulatorne prepreke koje usporavaju potpunu implementaciju digitalnih procesa. Na primer, Zakon o sprečavanju pranja novca zahteva fizičku prisutnost klijenata za identifikaciju prilikom otvaranja računa ili potpisivanja ugovora. Ova pravila otežavaju uvođenje potpunog digitalnog potpisivanja ugovora i otvaranja računa na daljinu. Neke banke, poput Telenor banke, razvile su alternativne metode, kao što je dostava dokumenata putem kurira, kako bi zaobišle ove prepreke.

<sup>34</sup> <https://rs.bloombergdria.com/>

Onlajn aplikacije za kredite razvijene su u 17 banaka u Srbiji, međutim, većina i dalje zahteva fizičku posetu filijalama radi potpisivanja ugovora, što usporava punu digitalizaciju kreditnog procesa. S druge strane, digitalni kanali kao što su internet i mobilno bankarstvo omogućavaju značajno smanjenje troškova obrade transakcija – prema procenama, od 1,3 do 7,8 puta u odnosu na tradicionalne transakcije obavljene u filijalama. Ovaj trend jasno motiviše banke da dodatno investiraju u unapređenje digitalnih platformi, u cilju smanjenja operativnih troškova i povećanja profitabilnosti (Stankić et al., 2023; Stefanovic et al., 2021).

Banke ulažu u razvoj veštačke inteligencije (AI) i analitiku velikih podataka kako bi unapredile personalizovane usluge i identifikovale obrasce u ponašanju korisnika. Implementacija ovih tehnologija omogućava brže i preciznije donošenje odluka, unapređuje upravljanje rizicima i smanjuje vreme obrade zahteva.

Banke u Srbiji ulažu u razvoj naprednih sistema zaštite podataka, uključujući enkripciju, višefaktorsku autentifikaciju i detekciju prevara.<sup>35</sup> Istovremeno, klijenti se sve više edukuju o bezbednom korišćenju digitalnih platformi, čime se povećava poverenje u digitalne usluge.

### **3.2 Uticaj digitalnih tehnologija na efikasnost poslovanja**

Digitalne tehnologije značajno unapređuju efikasnost poslovanja u bankarskom sektoru Srbije. Implementacija novih digitalnih rešenja omogućava brže i sigurnije obavljanje transakcija, smanjenje operativnih troškova i unapređenje korisničkog iskustva. Ova transformacija uključuje upotrebu elektronskog bankarstva, mobilnih aplikacija, veštačke inteligencije (AI), analitike velikih podataka i automatizovanih sistema za upravljanje procesima.

Većina banaka u Srbiji uvela je internet i mobilno bankarstvo, čime je omogućeno obavljanje transakcija u realnom vremenu. OTP banka beleži 85% rasta korisnika mobilnog bankarstva u poslednjih pet godina<sup>36</sup>, dok je UniCredit<sup>37</sup> banka povećala obim transakcija putem digitalnih kanala za 68% u 2022. Ove tehnologije unapredile su efikasnost pružanja usluga i omogućile veću

---

<sup>35</sup> OECD (2020) preporučuje stalnu edukaciju zaposlenih i korisnika o sajber pretnjama kako bi se povećala otpornost na napade, uključujući socijalni inženjering i fišing.

<sup>36</sup> <https://www.otpbanka.rs/o-nama/godisnji-izvestaji/>

<sup>37</sup> <https://www.unicreditbank.rs/rs/o-nama/izvestaji/finansijski.html>

dostupnost bankarskih proizvoda, posebno među mlađim korisnicima koji preferiraju digitalne kanale.

Uvođenje multifunkcionalnih bankomata i samouslužnih zona omogućava klijentima pristup bankarskim uslugama 24/7. ProCredit<sup>38</sup> banka je prva uvela ove zone, što je rezultiralo smanjenjem troškova poslovanja za 25% i povećanjem zadovoljstva klijenata. Erste banka<sup>39</sup> je zabeležila 40% smanjenje administrativnih troškova nakon implementacije automatizovanih procesa za upravljanje kreditima.

Banke u Srbiji koriste AI i analitiku velikih podataka kako bi analizirale ponašanje korisnika, identifikovale rizike i optimizovale ponudu proizvoda. AI alati omogućavaju personalizovane usluge, predviđanje potreba klijenata i automatsku obradu zahteva, čime se povećava preciznost i smanjuje vreme obrade. Raiffeisen<sup>40</sup> banka koristi AI za procenu kreditnog rizika, čime je smanjila vreme odobravanja kredita za 30%. UniCredit banka koristi analitiku podataka za segmentaciju klijenata, čime je povećala prodaju osiguranja za 18%.

Razvoj digitalnih platformi omogućava klijentima brz i jednostavan pristup informacijama i transakcijama. Banke nude aplikacije koje omogućavaju beskontaktna plaćanja, skeniranje čekova i upravljanje računima putem mobilnih uređaja. ProCredit banka beleži da se više od 95% transakcija obavlja digitalno, čime su smanjene gužve u filijalama i povećano zadovoljstvo korisnika. Takođe, NLB komercijalna banka<sup>41</sup> je zabeležila povećanje broja korisnika mobilnog bankarstva za 70% nakon unapređenja svojih aplikacija.

Onlajn aplikacije za kredite omogućavaju bržu obradu zahteva, pri čemu je 17 banaka u Srbiji razvilo ovakve sisteme. AI tehnologije smanjile su vreme obrade kredita za 50%, dok OTP banka nudi usluge predodobrenja kredita u roku od 15 minuta. Iako, većina banaka još uvek zahteva fizičko prisustvo za potpisivanje ugovora, ProCredit i Mobi<sup>42</sup> banka omogućavaju digitalno potpisivanje ugovora, čime dodatno smanjuju vreme čekanja i povećavaju efikasnost.

---

<sup>38</sup> <https://www.procreditbank.rs/o-nama/finansijski-izvestaji>

<sup>39</sup> <https://www.erstebank.rs/sr/o-nama/finansijski-izvestaji>

<sup>40</sup> <https://www.raiffeisenbank.rs/sr/common/izvestaji.html>

<sup>41</sup> <https://www.nlbkb.rs/o-nama/finansijski-izvestaji>

<sup>42</sup> <https://www.mobibanka.rs/sr/o-nama/mobi-banka/izvestaji/>

Analiza pokazuje snažnu korelaciju između investicija u digitalne tehnologije i profitabilnosti banaka. Pirsonov koeficijent korelacije ukazuje na srednje do snažne veze između ulaganja u nematerijalnu imovinu, poput softverskih rešenja, i neto dobiti banaka (Murinde et al., 2022). Halk banka<sup>43</sup> je zabeležila 22% rast dobiti nakon ulaganja u digitalnu infrastrukturu, dok je AIK banka<sup>44</sup> povećala profitabilnost za 19% zahvaljujući automatizaciji procesa.

Digitalne tehnologije omogućavaju bankama da se lakše takmiče sa *fintech* kompanijama i drugim nebankarskim pružaocima finansijskih usluga. Razvoj API tehnologija omogućava bankama integraciju sa trećim stranama, čime se povećava paleta usluga dostupnih korisnicima. OTP i UniCredit, već sarađuju sa globalnim platformama poput Apple Pay i Google Pay, omogućavajući klijentima brže i jednostavnije transakcije.

Digitalizacija smanjuje troškove poslovanja banaka automatizacijom procesa i smanjenjem potrebe za fizičkim filijalama. Banke poput NLB komercijalne banke zabeležile su smanjenje troškova poslovanja za 12%, dok je Erste banka smanjila troškove po transakciji za 7,8 puta u odnosu na filijale. Ova ušteda omogućava bankama preusmeravanje resursa na inovacije i razvoj novih proizvoda.

Implementacija višefaktorske autentifikacije, biometrijskih podataka i naprednih algoritama za detekciju prevara povećava bezbednost digitalnih transakcija. Banke ulažu u sajber bezbednost kako bi zaštitile podatke klijenata, čime jačaju poverenje korisnika u digitalne servise. Na primer, Raiffeisen banka je povećala sigurnost za 35% uvođenjem biometrijskih autentifikacija<sup>45</sup>, dok UniCredit koristi blokčejn tehnologiju za dodatnu zaštitu podataka.

Analizirajući ključne pokazatelje efikasnosti poslovanja, primetno je da digitalne usluge beleže značajan rast. Na primer, broj korisnika digitalnog bankarstva povećao se za 44% samo u 2022. godini, što ukazuje na rastuće poverenje u digitalne kanale. Korišćenje kartica i digitalnih kanala plaćanja takođe je u porastu, sa prosečnim godišnjim rastom kartičnog prometa od 15,6% u periodu

---

<sup>43</sup> <https://www.halkbank.rs/O-nama/Finansijski-izvestaji/Godisnji-Izvestaj-o-poslovanju.331.html>

<sup>44</sup> <https://aikbanka.rs/>

<sup>45</sup> Raiffeisen banka u Srbiji unapredila je komunikaciju s klijentima uvođenjem čet-bota Rea, zasnovanog na veštačkoj inteligenciji, koji omogućava brze i sigurne informacije putem Viber i Messenger platformi, čime je dodatno pojednostavila korišćenje i povećala efikasnost usluga.

od 2020. do 2023. godine.<sup>46</sup> Implementacija savremenih tehnologija, poput mobilnih plaćanja, NFC tehnologije i e-commerce platformi, doprinela je unapređenju efikasnosti poslovanja i jačanju konkurentnosti banaka. Digitalizacija je omogućila bankama da privuku nove klijente i unaprede svoju tržišnu poziciju. Banke koje su više ulagale u digitalizaciju postigle su bolje rezultate u pogledu broja transakcija i korisnika, čime su dodatno potvrdile značaj tehnoloških inovacija u unapređenju poslovanja.

### **3.3 Zadovoljstvo klijenata i korisničko iskustvo**

Digitalne tehnologije revolucionarno su promenile način na koji banke komuniciraju s klijentima, značajno unapređujući zadovoljstvo korisnika i kvalitet njihovog iskustva. Prema OECD-ovom izveštaju o digitalnim poremećajima u bankarstvu (2020), digitalizacija omogućava bankama da odgovore na sve zahtevnije potrebe klijenata, pružajući im personalizovane usluge i efikasnu podršku. Ovaj trend prati globalna težnja ka pojednostavljenju bankarskih usluga i povećanju njihove dostupnosti.

Najveće banke u Srbiji, poput Banca Intesa i AIK banke, aktivno koriste digitalne tehnologije kako bi poboljšale zadovoljstvo klijenata. Banca Intesa je implementirala napredne mobilne aplikacije koje omogućavaju korisnicima da brzo i jednostavno obavljaju transakcije, plaćaju račune i kontrolišu svoje finansije. Njihov sistem mobilnog bankarstva sadrži funkcije kao što su skeniranje računa za instant plaćanja, kreiranje šablona za ponavljajuće transakcije i digitalni sefovi za dokumente. AIK banka se fokusira na digitalnu transformaciju kroz personalizovane usluge i analitičke modele za predviđanje potreba klijenata. Korišćenjem algoritama mašinskog učenja, AIK banka pruža personalizovane preporuke i nudi prilagođene finansijske proizvode. Takođe, implementirali su blokčejn tehnologiju za unapređenje sigurnosti podataka, kao i čet-bot asistente za podršku korisnicima 24/7. Ove tehnologije omogućavaju povećanje poverenja korisnika kroz veću transparentnost, sigurnost i dostupnost usluga. Banke su primetile rast zadovoljstva klijenata, meren anketama i analizom recenzija, uz značajno smanjenje vremena potrebnog za obradu zahteva.

---

<sup>46</sup> <https://www.statista.com/>

Korisnici sada mogu u realnom vremenu da dobiju informacije o statusu transakcija i pristupe podršci, što poboljšava ukupno korisničko iskustvo. Istraživanje (Maksic et al., 2024) ukazuje da sociodemografski faktori, kao što su starost, obrazovanje i računarska pismenost, imaju ključnu ulogu u razumevanju zadovoljstva korisnika digitalnim uslugama. Istraživanje sprovedeno na uzorku od 145 korisnika u kome pokazuje da viši nivo obrazovanja i računarske pismenosti doprinosi većem zadovoljstvu korisnika digitalnim bankarskim uslugama, dok starije osobe i one s nižim prihodima češće iskazuju niži nivo zadovoljstva. Ovi nalazi ukazuju na potrebu za većim ulaganjima u digitalnu edukaciju i dostupnost kako bi se obezbedila ravnopravnost u pristupu savremenim bankarskim rešenjima (Maksic et al., 2024).

Jedan od ključnih faktora zadovoljstva klijenata je dostupnost bankarskih usluga u realnom vremenu. Prema (Pavithra & Geetha, 2021), automatizacija procesa i mobilne aplikacije omogućavaju korisnicima da obavljaju transakcije u bilo kojem trenutku, bez potrebe za fizičkom posetom filijalama. Banke u Srbiji, poput ProCredit-a i Raiffeisen-a, prednjače u implementaciji ovih tehnologija, omogućavajući klijentima jednostavan pristup uslugama putem multifunkcionalnih bankomata i digitalnih platformi.

Rad (Maksic et al., 2024) dodatno naglašava da su ključni elementi zadovoljstva korisnika efikasnost, sistemska dostupnost, ispunjenje očekivanja i privatnost. Dok mlađe generacije daju visoke ocene u svim kategorijama, stariji korisnici iskazuju zabrinutost za sigurnost i privatnost. Ovo ukazuje na potrebu prilagođavanja digitalnih rešenja različitim korisničkim profilima.

Dalje, prema studiji (Stefanovic et al., 2021), banke koje integrišu digitalne tehnologije u svoje poslovanje beleže značajno veću stopu zadovoljstva korisnika, zahvaljujući brznoj obradi zahteva i personalizovanim rešenjima. Na primer, OTP banka nudi aplikacije koje omogućavaju korisnicima da otvore račune, odobre im se krediti i upravljaju finansijama bez posete banci, čime smanjuju administrativne troškove i štede vreme klijenata.

Efikasnost korisničkog iskustva dodatno je unapređena primenom veštačke inteligencije i analitike podataka. (Klein, 1971) u svom modelu bankarskog poslovanja ističe da optimizacija operativnih procesa doprinosi većem zadovoljstvu korisnika, dok automatizovani sistemi smanjuju greške i povećavaju preciznost usluga. Banke poput UniCredit-a koriste AI alate za personalizaciju ponuda i predviđanje potreba klijenata.

Primeri iz Švedske (Häggqvist, 2019) pokazuju da su banke koje su usvojile digitalne modele poslovanja zabeležile značajno povećanje korisničkog angažmana i poverenja, što se ogleda u većem broju transakcija i većoj lojalnosti klijenata. Slično tome, srpske banke ulažu u sisteme zasnovane na podacima kako bi analizirale obrasce ponašanja korisnika i pružile rešenja prilagođena njihovim potrebama.

U radu (Maksic et al., 2024) takođe se ističe važnost regulatornog okvira i sigurnosnih mera za uspešnu digitalnu transformaciju. Politički i ekonomski faktori, uključujući stabilnost i zakonodavni okvir, utiču na razvoj digitalnih usluga. Uz odgovarajuće regulative i sigurnosne mere, banke mogu dodatno povećati poverenje korisnika i osigurati širu prihvaćenost digitalnih rešenja.

Smanjenje vremena čekanja i povećanje brzine obrade zahteva ključni su faktori za poboljšanje korisničkog iskustva. Prema (Do et al., 2022), digitalne tehnologije omogućavaju smanjenje vremena obrade kredita sa nekoliko dana na nekoliko minuta, čime se povećava zadovoljstvo klijenata i konkurentnost banke.

Digitalno korisničko iskustvo predstavlja celokupnu interakciju između korisnika i banke putem digitalnih kanala, kao što su mobilne aplikacije, internet bankarstvo i čet-bot alati. Erste banka je prepoznala značaj digitalne transformacije i inovacija u unapređenju korisničkog iskustva, čime je postala jedna od vodećih banaka u ovom segmentu u Srbiji. Implementacijom savremenih tehnoloških rešenja, banka omogućava brže, sigurnije i personalizovanije usluge, odgovarajući na rastuća očekivanja modernih korisnika.

Jedna od ključnih inovacija Erste banke je digitalna platforma „George“, koja korisnicima omogućava potpunu kontrolu nad finansijama na jednostavan i efikasan način. Ova aplikacija pruža personalizovane preporuke na osnovu analize prethodnih transakcija, omogućava kategorizaciju troškova i automatsko plaćanje računa. Platforma je osmišljena tako da olakša svakodnevno upravljanje finansijama, smanjujući potrebu za posetama filijalama i pružajući korisnicima veću fleksibilnost i kontrolu nad svojim sredstvima. Erste banka je takođe uvela čet-bot i virtuelne asistente kao moderne alate za komunikaciju sa korisnicima. Ove tehnologije omogućavaju brzo rešavanje problema, pružanje informacija u realnom vremenu i podršku pri obavljanju transakcija. Čet-bot alati koriste veštačku inteligenciju za prepoznavanje potreba

korisnika i pružaju odgovore koji su prilagođeni njihovim specifičnim zahtevima. Ova vrsta automatizovane podrške smanjuje opterećenje zaposlenih, a istovremeno poboljšava efikasnost i zadovoljstvo korisnika. Fokus na sigurnost jedan je od prioriteta Erste banke, koja koristi napredne tehnologije za zaštitu podataka i transakcija. Implementacija biometrijske autentifikacije, kao što su prepoznavanje lica i otiska prsta, uz dvofaktorsku verifikaciju, obezbeđuje visok nivo zaštite korisničkih informacija. Ove inovacije pružaju dodatni osećaj sigurnosti klijentima, omogućavajući im da sa poverenjem koriste digitalne usluge banke. Unapređenje internih procesa takođe igra ključnu ulogu u digitalnoj transformaciji Erste banke. Automatizacija *back-office*<sup>47</sup> operacija doprinosi bržoj obradi podataka, smanjenju administrativnih troškova i većoj tačnosti informacija. Ovi procesi omogućavaju efikasnije donošenje odluka, posebno kada je reč o odobravanju kredita, što značajno skraćuje vreme čekanja i poboljšava korisničko iskustvo. Analitički alati i analize velikih podataka omogućavaju Erste banci da bolje razume potrebe i navike svojih klijenata. Na osnovu prikupljenih podataka, banka nudi personalizovane preporuke i ciljana rešenja, kao što su programi štednje i finansijsko planiranje. Na primer, funkcija postavljanja ciljeva štednje omogućava korisnicima da automatski odvajaju sredstva za specifične potrebe, čime se dodatno unapređuje njihova finansijska disciplina. Erste banka kontinuirano prati povratne informacije korisnika kako bi unapredila postojeće usluge i razvila nove funkcionalnosti. Povratna sprega između inovacija i digitalnog korisničkog iskustva omogućava banci da brzo reaguje na promene u potrebama korisnika i implementira rešenja koja dodatno povećavaju njihovo zadovoljstvo. Na primer, na osnovu analize navika korisnika, banka je omogućila funkcije podsećanja na plaćanja i automatske obrade ponavljajućih transakcija, čime se dodatno povećava efikasnost i praktičnost.<sup>48</sup>

Najzad, digitalizacija bankarskog sektora u Srbiji rezultirala je povećanjem zadovoljstva korisnika, zahvaljujući personalizovanim uslugama, brzini obrade zahteva i sigurnosti transakcija. Banke ulažu u inovacije i nove tehnologije kako bi unapredile korisničko iskustvo i povećale

---

<sup>47</sup> Ovaj termin označava administrativne i tehničke funkcije unutar kompanije koje podržavaju osnovne poslovne aktivnosti, ali nisu direktno povezane sa klijentima. U bankarstvu, *back-office* obuhvata obradu transakcija, upravljanje rizicima, komplajans, IT podršku i računovodstvo. Komplajans (engl. *compliance*) označava usklađenost poslovanja sa zakonima, regulatornim zahtevima, internim pravilima i etičkim standardima. U bankarskom sektoru, ovo uključuje kontrolu poštovanja propisa protiv pranja novca, zaštite podataka, upravljanja rizicima i drugih oblasti koje regulišu rad finansijskih institucija.

<sup>48</sup> <https://www.erstebank.rs/sr/o-nama/finansijski-izvestaji>

konkurentnost. Znajući da se poverenje gradi godinama, a ruši za sekundu, time srpske banke nastoje da kroz digitalnu transformaciju održe poverenje klijenata i pruže vrhunsko iskustvo.

### **3.4 Unapređenje sigurnosti i konkurentnosti**

Digitalizacija bankarskog sektora u Srbiji nije samo odgovor na zahteve modernog tržišta, već i ključni faktor u unapređenju sigurnosti finansijskih transakcija i zaštiti podataka korisnika. Primena naprednih tehnologija, kao što su biometrijska autentifikacija, veštačka inteligencija (AI), blokčejn i analitika velikih podataka, omogućava bankama da efikasnije prepoznaju i preveniraju rizike, čime jačaju poverenje klijenata i osiguravaju stabilnost sistema.

Povećana upotreba digitalnih kanala povećava izazove u oblasti sajber bezbednosti. Banke u Srbiji ulažu u napredne sisteme zaštite podataka, uključujući enkripciju, višefaktorsku autentifikaciju, biometrijsku identifikaciju (otisak prsta, prepoznavanje lica i glasovna identifikacija) i detekciju prevara, čime se značajno smanjuje rizik od krađe identiteta i neovlašćenog pristupa. Ovi sistemi značajno smanjuju rizik od krađe identiteta i neovlašćenih pristupa. Prema OECD-u (2020), multifaktorska verifikacija predstavlja najefikasniji način zaštite digitalnih naloga jer kombinuje više slojeva sigurnosti.

Veštačka inteligencija i blokčejn tehnologija omogućavaju bankama kontinuirano praćenje transakcija u realnom vremenu, prepoznavanje prevara i preduzimanje preventivnih mera. OTP banka koristi AI za analizu podataka i blokiranje sumnjivih transakcija, dok UniCredit koristi blokčejn za bezbedno vođenje transakcija i ugovora, čime garantuje transparentnost i sigurnost. Ovaj pristup potvrđen je u istraživanjima (Milosevic et al., 2021) koji ističu da AI značajno doprinosi povećanju sigurnosti i efikasnosti poslovanja. Ova tehnologija prepoznata je kao ključni faktor u zaštiti podataka u istraživanju (Murinde et al., 2022).

Mobilne aplikacije, kao što su Intesa Mobi i *George Erste* banke, koriste naprednu enkripciju podataka i zaštitu koda aplikacija kako bi osigurale bezbednost čak i u slučajevima kompromitovanih uređaja. OECD (2020) naglašava da je ovakav pristup ključan u zaštiti mobilnih kanala, koji postaju dominantni oblik interakcije korisnika s bankama.

Robotizovani automatizacioni procesi (RPA) sistema u bankama poput OTP omogućavaju automatizaciju zadataka s visokim stepenom tačnosti, smanjujući rizik od ljudskih grešaka koje

često dovode do sigurnosnih propusta. Automatizacija doprinosi povećanju otpornosti na napade i ubrzava otkrivanje sumnjivih aktivnosti, što je potvrđeno istraživanjem (Mandic et al., 2014).

U srpskom bankarskom sektoru, praktična implementacija digitalizacije ogleda se kroz primenu naprednih tehnologija za unapređenje bezbednosti i efikasnosti. OTP banka koristi veštačku inteligenciju (AI) za prepoznavanje obrazaca prevara i robotizovanu automatizaciju procesa (RPA) kako bi smanjila greške u obradi podataka, osiguravajući visok nivo zaštite sistema. S druge strane, Banca Intesa primenjuje biometrijsku autentifikaciju i multifaktorsku verifikaciju, čime minimizira rizik od neovlašćenog pristupa. Erste banka, putem digitalne platforme *George*, omogućava sigurno otvaranje računa na daljinu, eliminisajući potrebu za fizičkim dolaskom u filijalu, dok UniCredit banka koristi blokčejn tehnologiju za zaštitu transakcija i ugovora, garantujući integritet podataka. Ove inovacije potvrđuju nalaze (Milosevic et al., 2021), koji ističu da primena digitalnih tehnologija značajno poboljšava sigurnost i operativnu efikasnost u bankarskom sektoru.

### **3.5 Primeri iz prakse i empirijsko istraživanje**

Digitalizacija u bankarstvu Srbije donosi brojne prednosti, uključujući povećanje efikasnosti, unapređenje sigurnosti, personalizaciju usluga, pristup bankarskim servisima u realnom vremenu i poboljšanje korisničkog iskustva. Automatizacija procesa, poput obrade kredita i verifikacije korisnika, značajno smanjuje operativne troškove i povećava tačnost transakcija, čime doprinosi profitabilnosti banaka (Mandic et al., 2014).

Automatizacija procesa, kao što su obrade kredita i verifikacija korisnika, smanjuje operativne troškove i povećava tačnost transakcija. Studije pokazuju da digitalizacija omogućava optimizaciju resursa i ubrzavanje procesa, što doprinosi većoj profitabilnosti banaka, a to potvrđuju rezultati istraživanja sprovedenih na bankama u Srbiji (Mandic et al., 2014).

Primena AI sistema za prepoznavanje sumnjivih transakcija i biometrijske autentifikacije smanjuje rizik od prevara i povećava sigurnost podataka. Banke u Srbiji, poput Banca Intesa i UniCredit, koriste ove tehnologije kako bi zaštitile podatke korisnika, što se poklapa sa nalazima međunarodnih studija o uticaju digitalizacije na bezbednost (Milosevic et al., 2021).

### 3.5.1 Primeri iz prakse

Banca Intesa predvodi digitalnu transformaciju u Srbiji. Njena aplikacija Intesa Mobi omogućava korisnicima da u realnom vremenu obavljaju transakcije, prate stanje računa i upravljaju finansijama.<sup>49</sup> Integracija biometrijske autentifikacije, poput otiska prsta i prepoznavanja lica, unapređuje sigurnost i smanjuje rizik od prevara, što je potvrđeno analizom finansijskih parametara banaka u Srbiji (Mandic et al., 2014).

Raiffeisen banka<sup>50</sup> koristi AI tehnologije za analizu kreditne sposobnosti klijenata, omogućavajući brzo odobravanje kredita i obradu podataka. Mobilna aplikacija nudi funkcionalnosti za budžetiranje i analizu potrošnje, pomažući korisnicima da bolje upravljaju finansijama, čime se povećava efikasnost i smanjuju operativni troškovi (Milosevic et al., 2021).

OTP banka<sup>51</sup> je implementirala RPA tehnologije za obradu kredita i otvaranje računa, čime su procesi postali efikasniji i pouzdaniji. Automatizovani sistemi smanjuju greške i povećavaju zadovoljstvo korisnika, dok čet-bot asistenti omogućavaju dostupnost podrške 24/7, što je dodatno naglašeno u istraživanjima o digitalnom bankarstvu (Khuong et al., 2022).

UniCredit<sup>52</sup> banka primenjuje klad tehnologije i naprednu analitiku za personalizaciju svojih usluga. Digitalni alati omogućavaju praćenje korisničkih navika i kreiranje prilagođenih ponuda, dok integracija elektronske dokumentacije smanjuje troškove i ubrzava poslovne procese. Ova praksa je u skladu sa globalnim trendovima koje je identifikovao OECD (2020) u analizi digitalnih poremećaja u bankarstvu.

Erste<sup>53</sup> banka razvila je platformu *George*, koja omogućava praćenje finansijskih trendova, planiranje budžeta i otvaranje računa na daljinu. Ova platforma koristi analitiku podataka za pružanje personalizovanih preporuka, čime povećava angažovanost korisnika i poboljšava upravljanje ličnim finansijama, što je dodatno potvrđeno u studijama o bankarskoj digitalizaciji (Murinde et al., 2022).

---

<sup>49</sup> <https://www.bancaintesa.rs/stanovnistvo/finansijski-izvestaji.html>

<sup>50</sup> <https://www.raiffeisenbank.rs/sr/common/izvestaji.html>

<sup>51</sup> <https://www.otpbanka.rs/o-nama/godisnji-izvestaji/>

<sup>52</sup> <https://www.unicreditbank.rs/rs/o-nama/izvestaji/finansijski.html>

<sup>53</sup> <https://www.erstebank.rs/sr/o-nama/finansijski-izvestaji>

Analitika podataka omogućava bankama da bolje razumeju potrebe korisnika i kreiraju prilagođene ponude. Erste banka, putem platforme *George*, nudi savete i preporuke na osnovu finansijskih navika korisnika, čime povećava angažovanost i zadovoljstvo klijenata, a takve prakse su prepoznate kao ključne za održivu konkurentsku prednost (Murinde et al., 2022).

Mobilne aplikacije i onlajn platforme omogućavaju korisnicima da brzo i jednostavno obavljaju transakcije, prate stanje na računima i upravljaju finansijama. Banke, uključujući Banca Intesa, Raiffeisen i Erste, nude ovakve servise, koji zadovoljavaju potrebe modernih korisnika, što potvrđuju globalne analize o očekivanjima korisnika (Khuong et al., 2022).

Korišćenjem AI čet-botova i digitalnih platformi za komunikaciju, banke pružaju bržu podršku korisnicima, smanjujući potrebu za fizičkim odlaskom u filijale. OTP banka prednjači u ovoj oblasti sa naprednim čet-bot asistentima, koji pružaju informacije 24/7 i poboljšavaju korisničku podršku, što je identifikovano kao ključna komponenta digitalne transformacije (OECD, 2020).

Primena veštačke inteligencije (AI) i biometrijske autentifikacije smanjuje rizik od prevara i povećava bezbednost podataka, što se posebno ističe kod banaka poput Banca Intesa i UniCredit (Milosevic et al., 2021). Analitika podataka omogućava kreiranje prilagođenih ponuda, kao što Erste banka čini putem platforme *George*, povećavajući angažovanost klijenata (Murinde et al., 2022). Korišćenje mobilnih aplikacija i onlajn platformi omogućava korisnicima pristup uslugama u realnom vremenu, zadovoljavajući savremene potrebe tržišta (Khuong et al., 2022). Takođe, upotreba AI čet-bota i digitalnih platformi, kao što je to implementirala OTP banka, omogućava brzu i efikasnu podršku klijentima, smanjujući potrebu za fizičkim odlaskom u filijale (OECD, 2020).

Digitalizacija u bankarskom sektoru Srbije nije samo trend, već imperativ za postizanje konkurentске prednosti. Uvođenje tehnologija kao što su AI, RPA, analitika podataka i klad sistemi omogućava bankama da unaprede efikasnost, povećaju bezbednost i pruže personalizovane usluge. Primeri vodećih banaka u Srbiji, poput Banca Intesa, OTP, Erste i Raiffeisen, potvrđuju uspeh digitalnih transformacija kroz povećanu operativnu efikasnost i zadovoljstvo korisnika. Kako digitalna ekonomija nastavlja da se razvija, banke koje usvoje inovativne tehnologije imaće značajnu prednost u dinamičnom i konkurentnom finansijskom okruženju, što je potvrđeno u brojnim istraživanjima (OECD, 2020).

### 3.5.2 Empirijsko istraživanje

Za potrebe ovog master rada sprovedeno je istraživanje o tome koliko je rasprostranjena primena mobilnog bankarstva, kakva su iskustva i osnovne bojazni korisnika prilikom korišćenja aplikacija mobilnog bankarstva, u koje svrhe se ove usluge najviše koriste, na koji način korisnici vrše plaćanja računa. Pored toga, istaženo je da li i koliko je važna primena interneta u poboljšanju odnosa sa klijentima za bankarsko poslovanje, koji su razlozi za (ne)korišćenje e-bankinga u matičnoj banci anketirane osobe, kao i da li se i u kojoj meri koristi digitalni novac i kriptovalute.

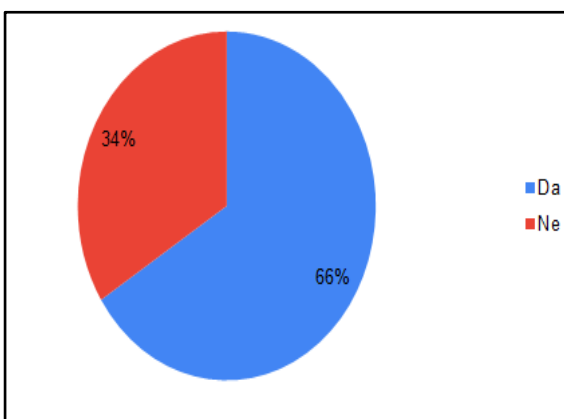
Anketa je pravljena uz pomoć Google forms aplikacije, rađena je tokom marta 2025. godine, sadržala je 21 pitanje, od kojih je 20 pitanja bilo zatvorenog tipa, odnosno imali su ponuđene odgovore i jedno pitanje je bilo otvorenog tipa. U anketi je učestvovalo 49 ispitanika i upitnik se nalazi u prilogu rada.

Cilj istraživanja je bio da se ispita stepen i zadovoljstvo korišćenja digitalnih bankarskih usluga, koje prednosti u korišćenju vide ispitanici, koji bi bili glavni rizici i nedostaci, te koje su preporuke ispitanika za poboljšanja ovih usluga. Rezultati istraživanja upravo mogu uticati na poboljšanje ovih usluga, kao i uvid u to koje bi rizike trebalo smanjiti kako bi se broj korisnika povećao.

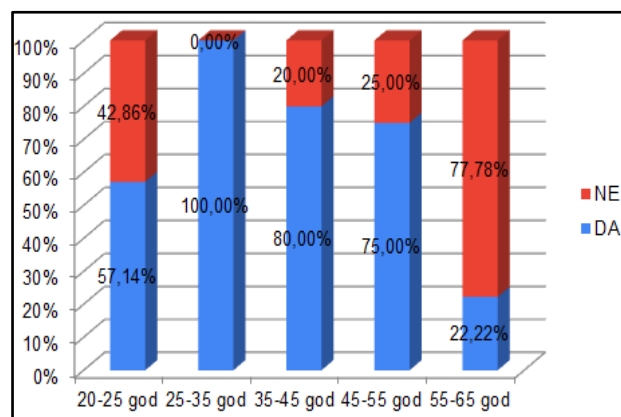
Uzorkom su obuhvaćeni ispitanici različitih polova, starosnih grupa, stepena stručne spreme i poslova na kojima su zaposleni što omogućava analizu uticaja različitih socijalnih i demografskih faktora na rezultate ankete. Dominantno ženski pol je preovladao u ovom uzorku sa 80%, ali na više pokazatelja se pokazalo da su procentualno odgovori na određena pitanja isti kod oba pola. Takođe, istraživanje je pokazalo da mesečni prihod nema direktnog uticaja na pokazatelje, jer su odgovori na pitanja u srazmeri po svim dodeljenim kriterijumima zarada. Starosna struktura ispitanika je 20-65 godina, što će biti od velike koristi prilikom prikaza rezultata i opšteg stava da starije generacije su više opredeljene „tradicionalnim“ načinima korišćenja bankarskih usluga. Nakon prikupljanja podataka, podaci su analizirani primenom osnovnih statističkih metoda, a radi boljeg pregleda, rezultati su prikazani i grafički.

Na slici 6. su prikazani odgovori ispitanika na pitanje da li koriste mobilno bankarstvo i podaci pokazuju da dve trećine ispitanika koristi. Ispitanici koji koriste usluge mobilnog bankarstva u 75% slučajeva to rade redovno, dok ostali to rade ili povremeno ili samo za pregled stanja na

računu. Prema starosnoj strukturi (Slika 7.), u populaciji 25-55 godina, preko 80% ispitanika koristi usluge mobilnog bankarstva, dok je kod najstarijih ispitanika taj broj manji od četvrtine. Ovim se potvrđuje opšte mišljenje da su starije generacije manje sklone novim tehnologijama, te da bankarske usluge koriste na način kako je to rađeno pre digitalizacije. U ovoj anketi nije bilo ispitanika koji su penzioneri, ali na osnovu dobijenih rezultata, pretpostavka je da je u toj grupi još niži procenat korisnika mobilnog bankarstva. Na osnovu ovoga, banke bi trebalo posebnu pažnju da obrate na ovu grupu klijenata, kako bi ih što više uputili i upozali sa prednostima i olakšicama koje korišćenje mobilnih platformi može doneti.

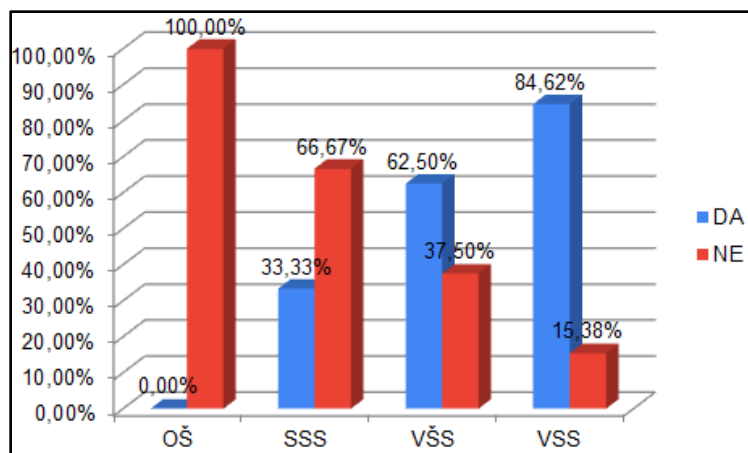


Slika 6: Korišćenje mobilnog bankarstva



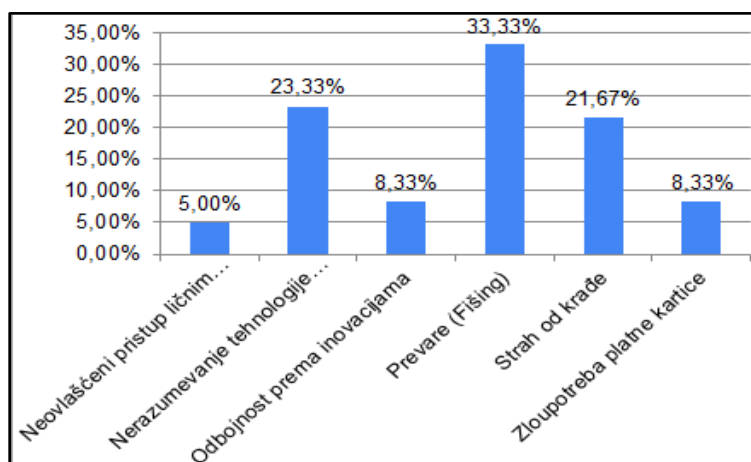
Slika 7: Korišćenje mobilnog bankarstva prema starosnoj strukturi

Rezultati ankete (Slika 8.) pokazuju da ispitanici sa višom ili visokom stručnom spremom u mnogo većem procentu koriste mobilno bankarstvo. To se može objasniti dosta boljom upućenošću, da li kroz obrazovanje ili posao, u sve prednosti koje donosi. Takođe, preko 70% ispitanika koristi mobilno bankarstvo više od dve godine i svi imaju visok stepen iskustva u korišćenju mobilnih telefona i aplikacija.



Slika 8: Korišćenje mobilnog bankarstva prema stepenu stručne spreme

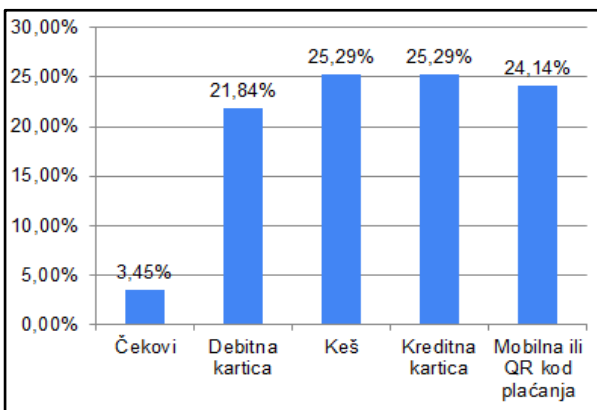
Kao glavni razlog nekorišćenja usluga mobilnog bankarstva (Slika 9.), trećina ispitanika je navela prevare, zatim nerazumevanje tehnologije i strah od krađe, dok su odbojnost prema inovacijama, zloupotreba kartica i neovlašćeni pristup ličnim podacima u dosta manjim procentima zastupljeni. Ovi pokazatelji mogu biti dobra osnova bankama na koje se rizike trebe posebno usredsrediti kako bi broj klijenata usluga mobilnog bankarstva bio uvećan.



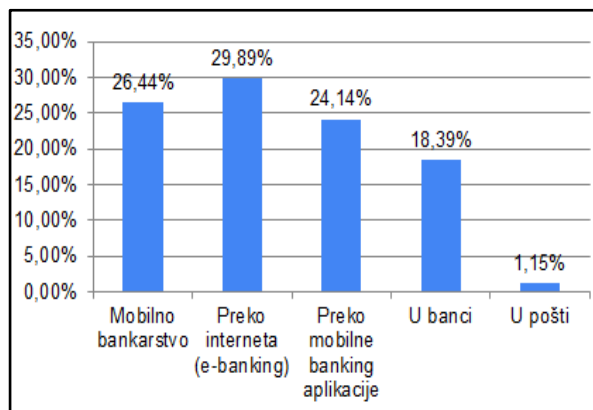
Slika 9: Razlozi za nekorišćenje mobilnog bankarstva

Istraživanje je pokazalo logičnu spregu da preko 70% ispitanika koji ne koriste mobilno bankarstvo svoje obaveze plaća u gotovu, dok ostalih 30% kreditnim i debitnim karticama. Nasuprot tome (Slika 10.), ispitanici koji koriste mobilno bankarstvo u gotovo identičnim procentima svoje obaveze plaćaju u gotovu, karticama i mobilnim ili QR kod plaćanjima, dok je mali procenat ispitanika naveo i čekove kao način plaćanja. Može se zaključiti da plaćanje u gotovu i dalje drži korak sa svim ostalim vidovima plaćanja, bez obzira na to što se korišćenjem mobilnog bankarstva

„na klik“ mogu vršiti plaćanja. Određeni finansijski stručnjaci smatraju da bi za držanje pod kontrolom mesečnih troškova najbolji način bio da se obaveze plaćaju u gotovu jer kartice čine novac apstrakcijom (Mori, 2021).



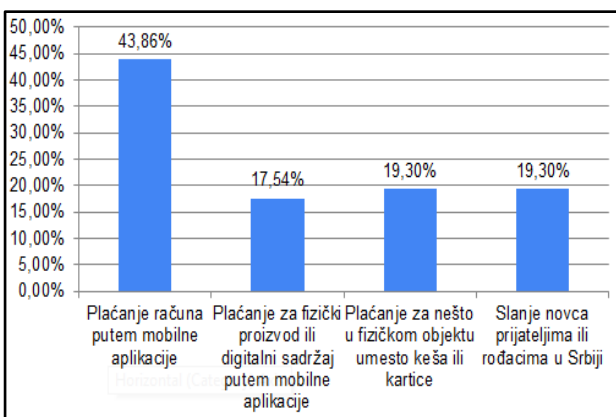
Slika 10: Sredstvo plaćanja korisnika mobilnog bankarstva



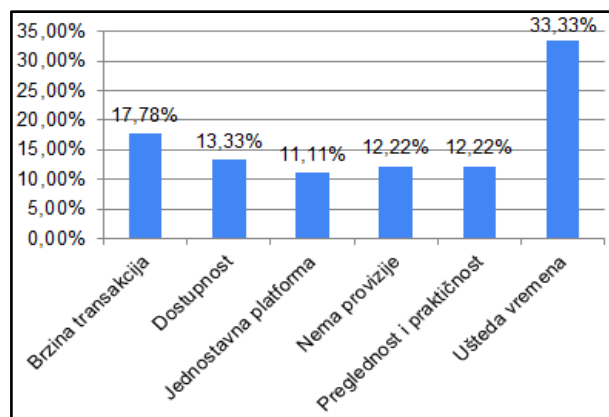
Slika 11: Način plaćanja korisnika mobilnog bankarstva

Interesantan pokazatelj je da preko 18% korisnika mobilnog bankarstva i dalje svoje obaveze plaća u banci (Slika 11.), a kao glavni razlog za to su nepotpuno razumevanje tehnologije i strah od prevare i krađe. Ipak, skoro 85% ispitanika smatra da je upotreba interneta važna u poboljšanju odnosa sa klijentima za bankarsko poslovanje. Ljudi sve više i više shvataju da bez interneta, efikasno poslovanje i komunikacija (i na nivou klijent-banka) je skoro pa nemoguća.

Kao glavni razlog odabira e-bankinga (Slika 12.), ispitanici navode plaćanje računa putem mobilne aplikacije, dok se sličan procenat ispitanika za to opredeljuje zbog plaćanja za proizvode i usluge putem aplikacije ili kao zamenu za keš i karticu, i za slanje novca u domaćem prometu. Kako se danas mnogo brže živi nego u prošlom veku, veoma je brži protok informacija i potrebno je mnogo napora izbalansirati poslovne i porodične obaveze, ispitanici su u najvećem procentu odabrali uštedu vremena (izbegavanje putovanja do određenog uplatnog mesta, čekanja u redovima i sl.), a zatim brzinu transakcija kao glavne inicijatore korišćenja mobilnog bankarstva. (Slika 13.)

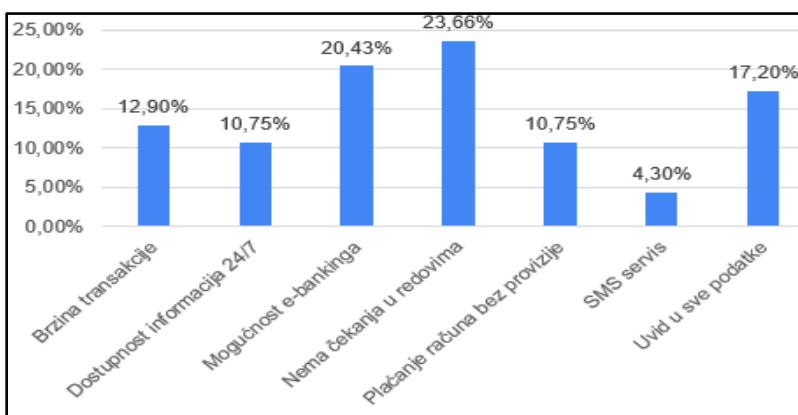


Slika 12: Razlog odabira e-bankinga



Slika 13: Najčešći razlozi korišćenja mobilnog bankarstva

Dodatna potvrda prethodnog zaključka ogleda se i u odgovorima koje su ispitanici dali na pitanje koji su najčešći razlozi zbog kojih se odlučuju na elektronsku platformu (Slika 14.), gde je skoro četvrtina ispitanika odgovorila da je to zbog izbegavanja čekanja u redovima. Mogućnost e-bankinga i uvid u sve podatke korisnika su sledeći kriterijumi po važnosti koji su navedeni.

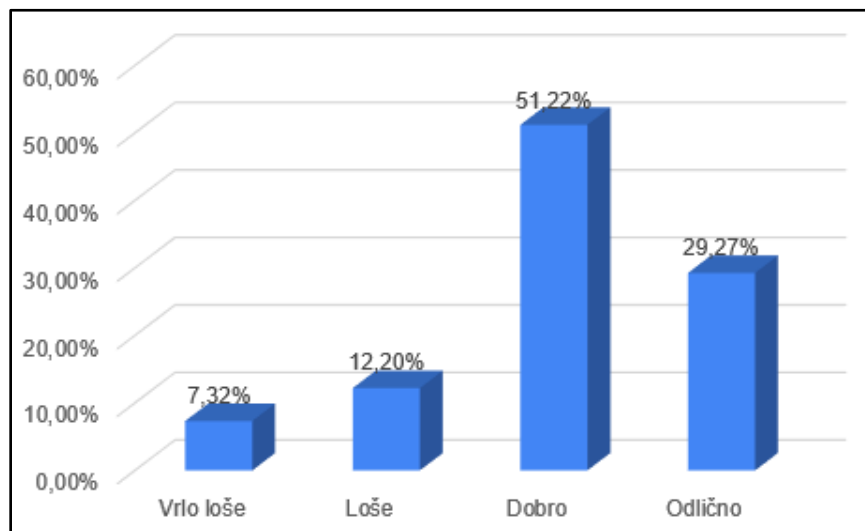


Slika 14: Najčešći razlozi korišćenja elektronske platforme

Istraživanje je pokazalo da korišćenje kriptovaluta i digitalnog novca nije još uvek u velikoj meri zastupljeno u našoj populaciji. Svega 12,77% ispitanika koristi ovakve vidove novca.

Iako digitalno bankarstvo donosi brojne prednosti i olakšanja korisnicima, rezultati ankete su pokazali da je svega 42,55% ispitanika veoma zadovoljno protokom informacija i brzinom transakcija na bankovnoj platformi, dok je oko 30% donekle zadovoljno. Ovo može biti bitan indikator na čemu bi trebalo raditi u budućnosti kako bi korisnici bili zadovoljniji. Slični procenti

zadovoljstva su dobijeni i analizom odgovora na pitanje koliko su ispitanici zadovoljni načinom komunikacije banke sa klijentima (telefon, imejlom, mobilnom aplikacijom ili putem digitalne platforme), veoma zadovoljan 38,29%, donekle zadovoljan 31,91%.



Slika 15: Zadovoljstvo uslugama mobilnog bankarstva

Na poslednjem dijagramu (Slika 15.) su prikazani rezultati ankete o zadovoljstvu korisnika uslugama mobilnog bankarstva. Evidentno je da je preko 80% korisnika zadovoljno uslugama usled svih prednosti koje su u radu navedene, a tiču se digitalizacije bankarskih usluga. Predlozi koje su određeni ispitanici naveli u cilju unapređenja usluga mobilnog bankarstva su pojednostavljenje aplikacija, pregled u koje svrhe se najviše troši novac, kao i veća transparentnost pri obavljanju plaćanja.

## **4 PREPORUKE ZA UNAPREĐENJE DIGITALNIH USLUGA U BANKARSTVU SRBIJE**

Unapređenje digitalnih usluga u bankarstvu Srbije ključno je za povećanje konkurentnosti banaka, efikasnije korišćenje resursa i bolje prilagođavanje potrebama korisnika. Optimizacija digitalnih procesa kroz primenu savremenih tehnologija, kao što su veštačka inteligencija, automatizacija i napredna analitika, omogućava ne samo bržu i kvalitetniju uslugu, već i viši nivo bezbednosti digitalnih transakcija. Dodatno, razvoj novih digitalnih rešenja doprinosi modernizaciji postojećih bankarskih sistema i pruža priliku za dalje inovacije, usklađene sa zahtevima savremenog digitalnog tržišta i promenjivim očekivanjima korisnika.

### **4.1 Strategije za optimizaciju digitalnih procesa**

Prvi korak u ovom procesu je primena veštačke inteligencije (AI), koja omogućava automatizaciju ponavljajućih zadataka, analizu velikih količina podataka i detekciju obrazaca u realnom vremenu. AI doprinosi većoj efikasnosti, smanjenju troškova i bržem reagovanju na promene na tržištu. Automatizovani algoritmi mogu se koristiti za analizu korisničkog ponašanja, prepoznavanje pretnji i personalizaciju usluga, čime se podiže nivo konkurentnosti banaka.

Druga ključna tehnologija je blokčejn koji omogućava kreiranje decentralizovanih sistema sa visokom transparentnošću transakcija i nepromenljivošću podataka. Ova tehnologija pomaže u sprečavanju prevara, povećava poverenje korisnika i pojednostavljuje procese verifikacije. Preporučuje se njeno postepeno uvođenje u ključne sektore digitalnog bankarstva, kao što su plaćanja i upravljanje ugovorima, radi povećanja sigurnosti i efikasnosti. Integracija blokčejn tehnologije u bankarskom sektoru u Srbiji je u povelju usled brojnih prednosti koje donosi, posebno u domenu sigurnosti i smanjenja troškova transakcija.

Istovremeno, banke bi trebalo da modernizuju postojeće sisteme kako bi poboljšale njihovu kompatibilnost sa novim digitalnim platformama. To podrazumeva migraciju sa zastarelih tehnologija na fleksibilne i skalabilne klad sisteme, kao i integraciju aplikacija koje omogućavaju besprekorno korisničko iskustvo. Digitalizacija operacija zahteva i razvoj naprednih sistema zaštite, uključujući dvofaktorsku autentifikaciju, biometrijsku identifikaciju i sisteme za detekciju pretnji u realnom vremenu. Banke bi trebalo da kontinuirano testiraju i unapređuju svoje bezbednosne protokole kako bi se nosile sa rastućim sajber pretnjama.

Dalje preporuke uključuju personalizovane usluge zasnovane na analizi podataka o korisnicima, čime se omogućava prilagođavanje ponuda individualnim potrebama. Intuitivne aplikacije sa personalizovanim funkcijama povećavaju angažovanost korisnika i njihovo zadovoljstvo. Pored tehnoloških unapređenja, banke treba da u fokusu imaju kontinuiranu edukaciju korisnika i zaposlenih kako bi bili spremni i imali veću sigurnost u korišćenju onlajn bankarskih usluge. Organizacija seminara, onlajn kurseva i vodiča o bezbednosnim protokolima i prednostima novih tehnologija može povećati poverenje u digitalne platforme i smanjiti rizik od zloupotrebe.

Kako bi osigurale brzinu i prilagodljivost u implementaciji novih rešenja, preporučuje se uvođenje fleksibilnih metodologija u razvoj digitalnih proizvoda. Ove metodologije omogućavaju brzo prilagođavanje promenama na tržištu kroz česte iteracije, testiranje i kontinuirano usavršavanje digitalnih rešenja. Banke treba da formiraju međufunkcionalne (engl. cross-functional) timove, sastavljene od stručnjaka iz različitih oblasti, koji mogu brzo donositi odluke, efikasno rešavati probleme i kontinuirano unapređivati postojeće sisteme. Paralelno sa tim, neophodno je redovno ažuriranje internih politika i procedura, što obezbeđuje usklađenost sa zakonskim i regulatornim zahtevima, bez usporavanja inovacija. Rezultati prethodno sprovedenih istraživanja (Maksic et al., 2024; OECD, 2020) ukazuju da regulatorni zahtevi često predstavljaju prepreku za brzu primenu inovacija, pa je neophodno unaprediti saradnju i komunikaciju između banaka i regulatornih tela kako bi se osiguralo pravovremeno prilagođavanje regulativi i smanjila pravna neizvesnost. U tom smislu, korišćenje tzv. regulatornih „sandbox“ platformi može dodatno olakšati implementaciju novih tehnologija u kontrolisanom regulatornom okruženju.

Digitalna transformacija zahteva i povećanu dostupnost usluga za sve korisničke grupe, uključujući osobe sa invaliditetom i stanovnike ruralnih područja. Razvoj pristupačnih aplikacija i edukativnih sadržaja prilagođenih specifičnim potrebama različitih korisnika ključan je za inkluzivnost digitalnih rešenja. Konačno, banke treba da implementiraju stalne procese praćenja i testiranja performansi digitalnih platformi kako bi osigurale njihovu pouzdanost, brzinu i bezbednost. Prikupljeni podaci mogu se koristiti za pravovremeno otkrivanje problema i optimizaciju funkcionalnosti sistema, čime se postiže kontinuitet u unapređenju digitalnih usluga.

Ove strategije za optimizaciju digitalnih procesa omogućavaju bankama u Srbiji da održe konkurentnost, povećaju sigurnost i efikasnost, kao i da unaprede korisničko iskustvo, istovremeno se prilagođavajući dinamičnim promenama na tržištu.

## **4.2 Poboljšanje korisničkog iskustva**

Poboljšanje korisničkog iskustva ključno je za povećanje zadovoljstva i lojalnosti, jer korisnici visoko vrednuju stabilnost sistema, jednostavnost korišćenja i sigurnost. Prvi korak u unapređenju korisničkog iskustva odnosi se na dizajn digitalnih platformi. Jasno strukturisane aplikacije sa intuitivnim menijima i personalizovanim sadržajem značajno olakšavaju korišćenje, dok tutorijali i vodiči pomažu korisnicima sa nižim nivoom digitalne pismenosti. Stabilnost i brzina sistema predstavljaju osnovu za pouzdanost, pa banke treba da ulože u modernizaciju tehnološke infrastrukture. Implementacija klauz tehnologija dodatno poboljšava fleksibilnost i dostupnost usluga, čime se minimizira rizik od zastoja i grešaka. Korisnici mogu biti nezadovoljni eventualnim sporim odzivom aplikacija i povremenim prekidima u radu sistema, što ukazuje na potrebu za konstantnim tehnološkim unapređenjima.

Sledeći aspekt odnosi se na personalizovane usluge koje koriste analitiku podataka i veštačku inteligenciju (AI) za kreiranje ponuda prilagođenih navikama i potrebama korisnika. Na primer, klijentima se mogu nuditi preporuke zasnovane na njihovim transakcijama, čime se povećava angažovanost i zadovoljstvo. Osim toga, integracija različitih kanala komunikacije, uključujući mobilne aplikacije, čet-botove, društvene mreže i kol centre, omogućava korisnicima da nesmetano prelaze sa jednog kanala na drugi, čime se osigurava kontinuitet u komunikaciji sa bankom. Veća integracija digitalnih usluga i brža reakciju banke na zahteve korisnika putem višekanalnih platformi bi trebalo pozitivno da utiču na korisničko zadovoljstvo.

Bezbednost i poverenje su ključni faktori u korišćenju digitalnih usluga, zbog čega se preporučuje implementacija multifaktorske autentifikacije, biometrijske verifikacije i enkripcije podataka. Transparentno obaveštavanje korisnika o merama zaštite dodatno jača poverenje i smanjuje zabrinutost. Banke bi trebalo da osiguraju i pristupačnost za sve korisnike, uključujući starije osobe i osobe sa posebnim potrebama. Obezbeđivanje većih fontova, glasovnih komandi i opcija za slabovidna lica značajno unapređuje inkluzivnost digitalnih platformi.

Tehnička podrška dostupna 24/7 putem više kanala, uključujući čet-botove sa AI funkcijama, obezbeđuje brzu pomoć korisnicima u slučaju problema. Takva podrška omogućava automatsko rešavanje jednostavnijih pitanja, dok složeniji zahtevi mogu biti prosleđeni stručnjacima. Redovno prikupljanje i analiza povratnih informacija putem anketa i ocena aplikacija pomažu bankama da identifikuju slabosti i unaprede svoje usluge. Ohrabrivanjem korisnika da daju predloge i komentare povećava se njihovo angažovanje i osećaj važnosti.

Edukovani korisnici bolje razumeju zaštitne mere i imaju više poverenja u digitalne sisteme, što dodatno doprinosi njihovom zadovoljstvu i lojalnosti. Banke treba da redovno prate performanse svojih digitalnih sistema kroz analizu korisničkih iskustava i testiranje novih funkcionalnosti. Na osnovu prikupljenih podataka mogu se sprovoditi inovacije koje omogućavaju održavanje konkurentnosti i visoke stope zadovoljstva korisnika. Stalna optimizacija, unapređenje sigurnosnih protokola i fleksibilna rešenja ključ su za dugoročni uspeh digitalnih usluga u bankarskom sektoru Srbije.

### **4.3 Povećanje bezbednosti digitalnih transakcija**

Povećanje bezbednosti digitalnih transakcija predstavlja ključni prioritet u modernizaciji bankarskog sektora Srbije. Kako bi se osigurala poverljivost, integritet i dostupnost podataka, preporučuje se primena sveobuhvatnih mera zaštite koje uključuju tehnička rešenja, regulatornu usklađenost i edukaciju korisnika. Povećanje bezbednosti digitalnih transakcija zahteva primenu tehničkih, regulatornih i edukativnih mera, uključujući AI i mašinsko učenje za analizu obrazaca ponašanja i prepoznavanje prevara, što omogućava zaštitu od neovlašćenog pristupa i zloupotreba. U kontekstu rastuće digitalizacije, bezbednost podataka postaje prioritet zbog sve učestalijih sajber pretnji i sofisticiranih napada. Implementacija modernih sigurnosnih tehnologija, poput dvofaktorske autentifikacije, enkripcije podataka i tokenizacije, ključna je za sprečavanje zloupotreba i očuvanje poverenja korisnika. Ove mere omogućavaju zaštitu transakcija u realnom vremenu i umanjuju rizik od prevara i gubitka podataka.

AI sistemi omogućavaju automatizovanu detekciju sumnjivih transakcija i trenutno obaveštavanje korisnika, čime se značajno povećava otpornost na napade. Integracija AI tehnologija u digitalne sisteme banaka omogućava brže reagovanje na pretnje, dok istovremeno smanjuje potrebu za manuelnim praćenjem i analizom podataka.

Blokčejn tehnologija, kao decentralizovana i nepromenljiva baza podataka, nudi dodatnu zaštitu transakcija kroz transparentnost i nemogućnost izmene podataka nakon njihove registracije. Ova tehnologija obezbeđuje visok nivo poverenja kod korisnika jer omogućava praćenje svih aktivnosti bez posrednika i smanjuje rizik od manipulacija. Njena primena u bankarstvu može dodatno unaprediti bezbednost plaćanja, posebno u prekograničnim transakcijama, gde se često javljaju problemi u praćenju i verifikaciji podataka.

Edukacija korisnika o bezbednosnim praksama, prepoznavanju fišing napada i zaštiti lozinki je ključna za smanjenje sajber pretnji i povećanje poverenja. Banke treba da ulažu u obuke i organizuju radionice, video tutorijale i onlajn kurseve kako bi korisnici bili spremniji za korišćenje naprednih funkcija i sigurnosnih mera. Svest korisnika o važnosti bezbednosti direktno utiče na smanjenje ranjivosti sistema, jer ljudski faktor često predstavlja najslabiju kariku u lancu zaštite. Osim toga, kontinuirana edukacija zaposlenih u bankama doprinosi jačanju unutrašnjih kapaciteta za prepoznavanje i reagovanje na pretnje.

Redovna testiranja bezbednosnih sistema, uključujući penetracione testove i simulacije napada, omogućavaju identifikaciju ranjivosti i pravovremeno unapređenje zaštitnih protokola. Ove provere pomažu u identifikaciji potencijalnih slabih tačaka i omogućavaju implementaciju efikasnih mera zaštite, čime se smanjuje rizik od sajber napada i gubitka podataka.

Usklađenost sa zakonskim i regulatornim okvirima predstavlja osnovu za sigurnost digitalnih transakcija. Banke moraju redovno pratiti promene u propisima i implementirati nove standarde kako bi osigurale usklađenost sa lokalnim i međunarodnim zakonima, uključujući GDPR. Takođe, potrebno je formirati timove za krizno upravljanje koji će brzo reagovati na incidente i pružiti podršku korisnicima. Pravovremeno informisanje klijenata o merama zaštite dodatno jača poverenje i smanjuje negativne posledice eventualnih napada.

Kombinacija savremenih tehnologija, kontinuirane edukacije i regulatorne usklađenosti ključna je za održavanje visokog nivoa bezbednosti digitalnih transakcija. Banke u Srbiji treba da nastave sa ulaganjem u istraživanje i razvoj, unapređenje softverskih rešenja i automatizaciju procesa kako bi bile korak ispred potencijalnih pretnji. Ove mere ne samo da unapređuju bezbednost, već i povećavaju konkurentnost bankarskog sektora, stvarajući poverenje korisnika i postavljajući temelje za održiv rast u digitalnoj eri.

#### **4.4 Predlozi za dalji razvoj digitalnih usluga**

Banke u Srbiji treba da nastave sa ulaganjem u inovacije kako bi unapredile efikasnost i bezbednost digitalnih usluga. Poseban fokus treba staviti na implementaciju veštačke inteligencije (AI) za analizu podataka i otkrivanje prevara, kao i na razvoj blokčejn tehnologija za povećanje transparentnosti i sigurnosti transakcija.

Banke treba da unaprede infrastrukturu, posebno u ruralnim područjima sa slabijim internet signalom, kako bi omogućile inkluzivniji pristup digitalnim uslugama. Razvoj mobilnih aplikacija koje funkcionišu i u uslovima niske povezanosti ključan je za širenje pristupa. Dodatno, banke bi trebalo da ponude specijalizovane opcije za starije korisnike i osobe sa invaliditetom, čime bi povećale pristupačnost i zadovoljstvo korisnika. Kao što je u sprovedenoj anketi utvrđeno, stariji korisnici su manje skloni novim tehnologijama iz različitih razloga, što naglašava potrebu za prilagođenim rešenjima.

Razvoj intuitivnih interfejsa i personalizovanih digitalnih rešenja treba da ostane prioritet. Banke treba da unaprede svoje aplikacije tako da korisnicima omoguće brži i jednostavniji pristup funkcijama, uz minimalan broj koraka za izvršenje transakcija. Korišćenje analitike korisničkog ponašanja može pomoći u prilagođavanju usluga specifičnim potrebama klijenata, čime se dodatno podstiče zadovoljstvo i lojalnost.

Programi obuke o digitalnim uslugama treba da budu dostupni svim korisnicima, sa naglaskom na zaštitu podataka i prepoznavanje prevara. Banke bi trebalo da organizuju radionice, video tutorijale i vebinare, kako bi korisnici bolje razumeli funkcionalnosti aplikacija i zaštitne mere koje im stoje na raspolaganju. Poseban fokus treba staviti na edukaciju starijih korisnika, koji su često manje upoznati sa digitalnim tehnologijama.

Banke treba da implementiraju napredne mere zaštite kao što su multifaktorska autentifikacija, biometrijska verifikacija i detekcija pretnji u realnom vremenu, uz redovno ažuriranje softverskih sistema i testiranje otpornosti na sajber napade. Pored toga, banke treba da povećaju transparentnost u vezi sa sigurnosnim merama i kriznim planovima, kako bi klijenti znali kako da reaguju u hitnim situacijama.

Prilagođavanje zakonskim regulativama mora biti kontinuiran proces. Banke treba da unaprede saradnju sa regulatornim telima radi bržeg usklađivanja sa novim standardima i zakonskim zahtevima. Implementacija novih pravila treba da prati ubranu digitalizaciju, kako bi se obezbedila fleksibilnost u primeni inovativnih tehnologija, bez ugrožavanja pravne sigurnosti.

Uvođenje naprednih sistema digitalnog identiteta, zasnovanih na biometriji i blokčejnu, može poboljšati sigurnost korisnika i pojednostaviti procese prijavljivanja. Ovi sistemi omogućavaju brže i bezbednije autentifikacije, smanjujući rizike od krađe identiteta i neovlašćenog pristupa podacima.

Razvoj sistema za brze i jeftine prekogranične transakcije može poboljšati konkurentnost srpskih banaka na globalnom nivou. Integracija sa međunarodnim sistemima plaćanja i primena digitalnih valuta centralnih banaka (engl. CBDC) omogućila bi efikasnije obavljanje transakcija, smanjenje troškova i veću transparentnost. Kako bi se povećao interes korisnika za digitalne valute, neophodno ih je dodatno informisati o prednostima i načinu korišćenja.

Saradnja sa *fintech* kompanijama može ubrzati digitalnu transformaciju i omogućiti bržu implementaciju inovativnih rešenja. Banke bi trebalo da razmotre zajedničke projekte sa tehnološkim startupima kako bi razvile napredne platforme za plaćanja, digitalne novčanike i aplikacije sa proširenim funkcijama.

## ZAKLJUČAK

Digitalizacija bankarstva u Srbiji predstavlja ključnu komponentu modernizacije finansijskog sektora i unapređenja korisničkog iskustva. Digitalne tehnologije omogućavaju brže transakcije, personalizovane ponude i optimizaciju poslovnih procesa, što doprinosi povećanju zadovoljstva korisnika i jačanju konkurentnosti banaka na tržištu.

Razvoj digitalnih platformi otvorio je nove mogućnosti za pružanje usluga koje su fleksibilnije, pristupačnije i prilagođene individualnim potrebama klijenata. Banke u Srbiji su prepoznale potrebu za digitalnom transformacijom kako bi se održala konkurentnost u globalizovanom okruženju i odgovorilo na rastuće zahteve korisnika za efikasnim i sigurnim rešenjima. Glavni problemi identifikovani su u domenu bezbednosti podataka, regulatornih zahteva i tehničke kompatibilnosti sistema. Ovi faktori usporavaju tempo implementacije novih tehnologija, ali istovremeno podstiču razvoj novih strategija za optimizaciju procesa i zaštitu korisnika.

Preporučeno je uvođenje naprednih sigurnosnih rešenja, kao što su biometrijska autentifikacija, multifaktorska verifikacija i blokčejn tehnologije, radi zaštite korisničkih podataka i smanjenja rizika od prevara. Istaknuta je potreba za kontinuiranim unapređenjem sigurnosnih protokola i većom transparentnošću kako bi se povratilo i zadržalo poverenje korisnika. Pored toga, istaknuta je važnost edukacije korisnika o prepoznavanju potencijalnih pretnji i pravilnom korišćenju digitalnih platformi.

Sprovedena anketa za potrebe ovog rada pokazala je da preko dve trećine ispitanika koristi usluge mobilnog bankarstva, od čega tri četvrtine to redovno radi, a kao glavni razlozi se navode ušteda vremena i brzina transakcija, što je u potpunom skladu koje trenutni način života nalaže. Kao aktivni korisnici su uglavnom ljudi mlađe starosne dobi, te bi banke trebalo da obrate dodatnu pažnju na približavanje i adaptaciju ovog načina pružanja usluga i najstarijim korisnicima. Takođe, visoko obrazovane osobe u drastično većem procentu koriste usluge mobilnog bankarstva u odnosu na osobe niže ili srednje stručne spreme. Ovo bi trebalo da bude indikator bankama za dodatnu edukaciju korisnika i olakšavanje upotrebe aplikacija. Dodatni input ovoj preporuci bi bio i to što su, pored prevara i straha od krađe, ispitanici naveli nerazumevanje tehnologije kao jedan od ključnih faktora rizika prilikom korišćenja usluga mobilnog bankarstva.

Kada je reč o hipotezi rada, koja je glasila: „Digitalne tehnologije značajno poboljšavaju operativne procese, sigurnost i zadovoljstvo klijenata, doprinoseći konkurentnosti sektora”, analiza je potvrdila njenu validnost. Podaci iz istraživanja ukazuju da digitalizacija pozitivno utiče na sve navedene aspekte, ali i da postoje prostori za dalja unapređenja kroz ulaganja u inovacije i regulatorna prilagođavanja.

Preporuke za dalji razvoj digitalnih usluga uključuju integraciju novih tehnologija poput veštačke inteligencije i automatizovanih sistema, jačanje saradnje sa *fintech* kompanijama i povećanje pristupačnosti usluga za sve korisničke grupe. Dodatno, potrebno je nastaviti istraživanje o dugoročnim efektima digitalizacije na bankarski sektor i prilagoditi strategije prema globalnim trendovima.

Rad je istakao da digitalne tehnologije nisu samo alat za modernizaciju bankarskih usluga, već i strateški faktor za održiv rast i konkurentnost u savremenom poslovnom okruženju. Implementacija predloženih strategija može doprineti daljem razvoju bankarskog sektora u Srbiji, omogućavajući mu da ostane konkurentan na globalnom tržištu i odgovori na sve veće zahteve korisnika.

## LITERATURA

- 1) Baskerville, R., Capriglione, F., & Casalino, N. (2020). Impacts, challenges, and trends of digital transformation in the banking sector. *Law and Economics Yearly Review Journal - LEYR*, 9(2), 341–362. Queen Mary University, London, UK. <https://ssrn.com/abstract=3835433>
- 2) Budler, M., Župič, I., & Trkman, P. (2021). The development of business model research: A bibliometric review. *Journal of Business Research*, 135, 480–495. <https://doi.org/10.1016/j.jbusres.2021.06.045>
- 3) Davies, R. (2020, December 10). Cyberattacks: Analysing resilience strategies of Bank of England.FDE-1. <https://www.financedirectoreurope.com/analysis/cyberattacks-analysing-resilience-strategies-bank-of-england/?cf-view>
- 4) Demkovich, A. (2023). Endogena intoksikacija u razvoju eksperimentalnog parodontitisa bakterijsko-imunog porekla. *Folia Medica*, 65(1), 149-154. <https://doi.org/10.3897/folmed.65.e71970>
- 5) Deutsche Bank. (2020). Risk deep dive: June 18, 2020. Deutsche Bank. [https://annualreport.deutsche-bank.com/files/documents/other-presentations-and-events/18\\_June\\_2020\\_Risk\\_Deep\\_Dive\\_vFinal1.pdf?language\\_id=1](https://annualreport.deutsche-bank.com/files/documents/other-presentations-and-events/18_June_2020_Risk_Deep_Dive_vFinal1.pdf?language_id=1)
- 6) Do, T. D., Pham, H. A. T., Thalassinou, E. I., & Le, H. A. (2022). The impact of digital transformation on performance: evidence from Vietnamese commercial banks. *Journal of Risk and Financial Management*, 15(1), 21. <https://doi.org/10.3390/jrfm15010021>
- 7) Doran, N. M., Bădîrcea, R. M., & Manta, A. G. (2022). Digitization and Financial Performance of Banking Sectors Facing COVID-19 Challenges in Central and Eastern European Countries. *Electronics*, 11(21), 3483. <https://doi.org/10.3390/electronics11213483>
- 8) Ekinici, R. (2021). The impact on digitalization on financial sector performance. In *The Impact of Artificial Intelligence on Governance, Economics and Finance*, vol. I, pp. 99–119. [https://doi.org/10.1007/978-981-33-6811-8\\_6](https://doi.org/10.1007/978-981-33-6811-8_6)
- 9) Elsaid, H. M. (2023). A review of literature directions regarding the impact of *fintech* firms on the banking industry. *Qualitative Research in Financial Markets*, 15(5), 693-711. <https://doi.org/10.1108/QRFM-10-2020-0197>
- 10) European Parliament. (2024). Measures for a high level of public sector interoperability across the Union (Interoperable Europe Act): European Parliament legislative resolution of 6 February 2024 on the proposal for a regulation of the European Parliament and of the Council laying down measures for a high level of public sector interoperability across the Union (COM(2022)0720 – C9-0387/2022 –

- 2022/0379(COD)) (P9\_TA(2024)0060). Official Journal of the European Union, C/2024/6351.  
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52024AP0060>
- 11) Federal Trade Commission. (2021). Consumer Sentinel Network data book 2021. Federal Trade Commission. [https://www.ftc.gov/system/files/ftc\\_gov/pdf/21apr\\_22-23app.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/21apr_22-23app.pdf)
  - 12) Fernández-Villaverde, J., & Sanches, D. R. (2019). Can currency competition work? *Journal of Monetary Economics*, 106, 1–15. <https://doi.org/10.1016/j.jmoneco.2019.07.003>
  - 13) Häggqvist, J. (2019). Digital transformation in the Swedish banking sector (Master's thesis, KTH Royal Institute of Technology, Stockholm, Sweden). KTH Industrial Engineering and Management. <https://www.diva-portal.org/smash/record.jsf?pid=diva2:1372205>
  - 14) Hodula, M. (2022). Does Fintech credit substitute for traditional credit? Evidence from 78 countries. *Financial Research Letters*, 46, 102469. <https://doi.org/10.1016/j.frl.2021.102469>
  - 15) Khuong, N. V., Phuong, N. T. T., Liem, N. T., Thuy, C. T. M., & Son, T. H. (2022). Factors affecting the intention to use financial technology among Vietnamese youth: Research in the time of COVID-19 and beyond. *Economies*, 10(3), 57. <https://doi.org/10.3390/economies10030057>
  - 16) Klein, M.A. (1971). A theory of the banking firm. *Journal of Money, Credit and Banking*, 3(2), 205-218. <https://doi.org/10.2307/1991279>
  - 17) Maksic, K., Golitsis, P., Radev, L., & Gkasis, P. (2024). Impact of Digitalization on Serbian Banking: Social Factors and Customer Satisfaction. *Theoretical Economics Letters*, 14, 2000-2035. <https://doi.org/10.4236/tel.2024.145100>
  - 18) Mandic, K., Delibasic, B., Knezevic, S., & Benkovic, S. (2014). Analysis of the financial parameters of Serbian banks through the application of the fuzzy AHP and TOPSIS methods. *Economic Modelling*, 43, 30–37. <https://doi.org/10.1016/j.econmod.2014.07.036>
  - 19) Milošević, N., Dobrota, M., Barjaktarović Rakočević, S. (2018). Digital economy in Europe: Evaluation of countries' performances. *Zbornik radova Ekonomskog fakulteta u Rijeci: časopis za ekonomsku teoriju i praksu*, 36(2), 861–880. <https://doi.org/10.18045/zbefri.2018.2.861>
  - 20) Milosevic, N., Dobrota, M., Dmitrovic, V., & Barjaktarovic Rakocevic, S. (2021). Managerial perception of human capital, innovations, and performance: evidence from the banking industry. *Engineering Economics*, 32(5), 446–458. <https://doi.org/10.5755/J01.EE.32.5.26032>
  - 21) Mori, S. (2021). *Finansijski kompas*, Atlantik bb. ISBN 978-99955-38-60-6

- 22) Murinde, V., Rizopoulos, E., & Zachariadis, M. (2022). The impact of the *Fintech* revolution on the future of banking: Opportunities and risks. *International Review of Financial Analysis*, 81, 102103. <https://doi.org/10.1016/j.irfa.2022.102103>
- 23) OECD. (2020). Digital Disruption in Banking and its Impact on Competition. [https://www.oecd.org/en/publications/digital-disruption-in-banking-and-its-impact-on-competition\\_b8d8fcb1-en.html](https://www.oecd.org/en/publications/digital-disruption-in-banking-and-its-impact-on-competition_b8d8fcb1-en.html)
- 24) Osterwalder, A., Pigneur, Y., & Tucci, C. (2005). Clarifying business models: Origins, present, and future of the concept. *Communications of the Association for Information Systems*, 16, 1-25. <https://doi.org/10.17705/1CAIS.01601>
- 25) Pavithra, C. B., & Geetha, K. (2021). Factors affecting customers' perception towards digital banking services. *Turkish Journal of Computer and Mathematics Education; Gurgaon*, 12(11), 1608–1614. <https://pdfs.semanticscholar.org/4555/1d95e18383d33a81e1455426f0aaa17f76a0.pdf>
- 26) PWC. (2016). Customers in the spotlight: How Fintech is reshaping banking, *Global Fintech Survey*. <https://www.pwc.com/gx/en/financial-services/fintech/assets/fin-tech-banking-2016.pdf>
- 27) Revathi, P. (2019). Digital banking challenges and opportunities in India. *EPRA International Journal of Economic Business Review*, 7(12), 20-23
- 28) Sayed, G., & Sayed, N.S. (2020). Customer experience with digital banking—a comparative study of private and public sector banks. *Productivity*, 61(1), 19–33
- 29) Schmidt-Jessa, K. (2023). The impact of COVID-19 on digital-only banks: Are they winners or losers? *Journal of Banking Regulation*, 24, 310–320. <https://doi.org/10.1057/s41261-022-00198-0>
- 30) Shahid, S., Islam, J. U., Malik, S., & Hasan, U. (2022). Examining consumer experience in using m-banking apps: A study of its antecedents and outcomes. *Journal of Retailing and Consumer Services*, 65, 102870. <https://doi.org/10.1016/j.jretconser.2021.102870>
- 31) Šimberová, I., & Kita, P. (2020). New business models based on multiple value creation for the customer: A case study in the chemical industry. *Sustainability*, 12(9), 3932. <https://doi.org/10.3390/su12093932>
- 32) Stankić, R. (2021). *Elektronsko poslovanje* (4. izd.). Ekonomski fakultet Univerziteta u Beogradu ISBN: 978-86-403-1699-6
- 33) Stankić, R., Lukić, V., & Popović, S. (2023). *Elektronski platni sistemi*. Ekonomski fakultet Univerziteta u Beogradu. ISBN: 978-86-403-1778-8

- 34) Stefanovic, N., Barjaktarovic, L., & Bataev, A. (2021). Digitainability and financial performance: Evidence from the Serbian banking sector. *Sustainability*, 13(23), 13461. <https://doi.org/10.3390/su132313461>
- 35) Svetski ekonomski forum. (2018). The Global Competitiveness Report 2018. World Economic Forum. <https://www.weforum.org/publications/the-global-competitiveness-report-2018/>
- 36) Vives, X. (2019). Digital Disruption in Banking. *Annual Review of Financial Economics*, 11(1), 243–272. <https://doi.org/10.1146/annurev-financial-100719-120854>

#### **VEB IZVORI:**

<https://aikbanka.rs/>  
[https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age\\_en](https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en)  
<https://digital-finance-platform.ec.europa.eu/>  
<https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation>  
<https://id4d.worldbank.org>  
<https://rs.bloombergadria.com/>  
<https://www.bancaintesa.rs/stanovnistvo/finansijski-izvestaji.html>  
<https://www.ecb.europa.eu/>  
[https://www.ecb.europa.eu/euro/digital\\_euro/html/index.en.html](https://www.ecb.europa.eu/euro/digital_euro/html/index.en.html)  
[https://www.eiopa.europa.eu/digital-operational-resilience-act-dora\\_en](https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en)  
<https://www.enisa.europa.eu/>  
<https://www.erstebank.rs/sr/o-nama/finansijski-izvestaji>  
<https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica>  
<https://www.europarl.europa.eu/>  
<https://www.halkbank.rs/O-nama/Finanskijski-izvestaji/Godisnji-Izvestaj-o-poslovanju.331.html>  
<https://www.mckinsey.com/>  
<https://www.mobibanka.rs/sr/o-nama/mobi-banka/izvestaji/>  
<https://www.nlbkb.rs/o-nama/finansijski-izvestaji>  
<https://www.otpbanka.rs/o-nama/godisnji-izvestaji/>  
<https://www.procreditbank.rs/o-nama/finansijski-izvestaji>  
<https://www.raiffeisenbank.rs/sr/common/izvestaji.html>  
<https://www.statista.com/>  
<https://www.unicreditbank.rs/rs/o-nama/izvestaji/finansijski.html>

## **SPISAK KORIŠĆENIH SKRAĆENICA**

2FA - Two-Factor Authentication

AI - Artificial intelligence

API - Application Programming Interface

ATM - Automated Teller Machine

BNPL - Buy Now, Pay Later

CBDC - Central Bank Digital Currency

CIA - Confidentiality, Integrity, Availability

DDoS - Distributed Denial of Service

DeFi - Decentralized finance

DFB - Digital Full Bank

DLP - Data Loss Prevention

DLT - Distributed Ledger Technology

DNS - Domain Name System

DORA - Digital Operational Resilience Act

DWB - Digital Wholesale Bank

ECB - European Central Bank

ECDSA - Elliptic Curve Digital Signature Algorithm

EEA - European Economic Area

e-KYC - electronic Know Your Customer

ENISA - European Network and Information Security Agency

FCA - Financial Conduct Authority

FTC - Federal Trade Commission

GDPR - General Data Protection Regulation

IMPS - Immediate Payment Service

IoT - Internet of Things

IPFS - InterPlanetary File System

MAS - Monetary Authority of Singapore

MFA - Multi-Factor Authentication

MiCA - Markets in Crypto-Assets Regulation

MITM - Man-In-The-Middle

ML - Machine Learning  
MSP - Mala i Srednja Preduzeća  
MST - Magnetic Secure Transmission  
NEFT - National Electronic Funds Transfer  
NFC - Near Field Communication  
OECD - Organisation for Economic Co-operation and Development  
P2P - Peer-To-Peer  
PIN - Personal Identification Number  
POS - Point of Sale  
PoS - Proof-of-Stake  
PoW - Proof-of-Work  
PSD2 - Payment Services Directive 2  
PSP - Payment Service Provider  
QR - Quick Response  
RPA - Robotic Process Automation  
RSA - Rivest–Shamir–Adleman  
RTGS - Real Time Gross Settlement  
SEPA - Single Euro Payments Area  
SME - Small and medium-sized enterprises  
SMS - Short Message Service  
SSL - Secure Sockets Layer  
SWIFT - Society for Worldwide Interbank Financial Telecommunications  
UPI - Unified Payments Interface  
ZKP - Zero-Knowledge Proof

## **PRILOG: UPITNIK**

- 1) Pol: a) M b) Ž
- 2) Starost: a) 20-25 b) 25-35 c) 35-45 d) 45-55 e) 55-65 f) >65
- 3) Stručna sprema: a) OŠ b) SSS c) VŠŠ d) VSS e) Drugo
- 4) Zanimanje: a) Profesor b) Administrativni radnik c) Vojno lice d) Zdravstveni radnik e) Penzioner f) Student g) Preduzetnik h) Nezaposlen j) Ostalo
- 5) Mesečni prihodi: a) Do 30.000 dinara b) Između 30.000 i 50.000 dinara c) Između 50.000 i 70.000 dinara d) Između 70.000 i 80.000 dinara e) Preko 80.000 dinara
- 6) Koji je najčešći način kojim plaćate? a) Keš b) Debitna kartica c) Kreditna kartica d) Čekovi e) Mobilna ili QR kod plaćanja
- 7) Da li koristite mobilno bankarstvo? a) DA b) NE
- 8) Iskustvo u korišćenju mobilnog bankarstva: a) Ne koristim b) Do 1 godine c) 1–2 godine d) Više od 2 godine
- 9) Iskustvo u korišćenju mobilnih telefona: a) Početnik b) Srednji nivo c) Iskusan
- 10) Na koji način plaćate račune? a) Preko mobilne banking aplikacije b) Preko interneta (e-banking) c) U banci d) U pošti
- 11) Razlozi nekorisćenja mobilnog bankarstva? a) Nerazumevanje tehnologije (softvera) b) Odbojnost prema inovacijama c) Strah od krađe d) Prevare (Fišing) e) Zloupotreba platne kartice f) Neovlašćeni pristup ličnim podacima g) Nemam stav
- 12) Koliko je važna primena Interneta u poboljšanju odnosa sa klijentima za bankarsko poslovanje? a) Vrlo važna b) Srednje važna c) Ne toliko važna d) Nevažna e) Nemam stav
- 13) Zbog čega biste odabrali e-banking kod Vaše banke? a) Slanje novca prijateljima ili rođacima u Srbiji b) Plaćanje za nešto u fizičkom objektu umesto keša ili kartice c) Plaćanje za fizički proizvod ili digitalni sadržaj putem mobilne aplikacije d) Plaćanje računa putem mobilne aplikacije e) Nemam stav
- 14) U kojoj meri ste zadovoljni sa protokom informacija i brzinom transakcija na bankovnoj platformi Vaše banke? a) Veoma zadovoljan b) Donekle zadovoljan c) Nemam stav d) Donekle nezadovoljan e) Veoma nezadovoljan

- 15) Koliko ste zadovoljni načinom komunikacije Vaše banke sa klijentima (telefon, imejlom, mobilnom aplikacijom ili putem digitalne platforme? a) Veoma zadovoljan b) Donekle zadovoljan c) Nemam stav d) Donekle nezadovoljan e) Veoma nezadovoljan
- 16) Koliko često koristite usluge mobilnog bankarstva? a) Redovno b) Povremeno c) Retko d) Samo za pregled stanja na računu e) Nemam stav
- 17) Koji su razlozi korišćenja mobilnog bankarstva? a) Ušteda vremena b) Jednostavna platforma c) Brzina transakcija d) Nema provizije e) Preglednost i praktičnost f) Dostupnost g) Nemam stav
- 18) Razlozi zbog kojih su se ispitanici odlučili za elektronsku platformu: a) Mogućnost e-bankinga b) Brzina transakcije c) Plaćanje računa bez provizije d) SMS servis e) Uvid u sve podatke f) Nema čekanja u redovima g) Dostupnost informacija 24/7 h) Nemam stav
- 19) Koliko ste zadovoljni uslugama mobilnog bankarstva? a) Nemam stav b) Vrlo loše c) Loše d) Dobro e) Odlično
- 20) Da li koristite digitalni novac i kriptovalute? a) DA b) NE
- 21) Predlozi za unapređenje bankarskih usluga u Vašoj banci?
- 

Višestruki odgovori dozvoljeni su u pitanjima: 6, 10, 11, 13, 17, 18.