

Sigurnije financije: Kako AI, IoT i Blockchain revolucioniraju digitalnu sigurnost

Zoran Čekerevac^a, Petar Čekerevac^b

^a Prof. dr. sc., dipl. ing. stroj., samostalni istraživač, Beograd, Srbija, zoran@cekerevac.eu

^b Mag. rel. int., samostalni istraživač, Beograd, Srbija, petar.cekerevac@gmail.com

Sažetak

Integracija umjetne inteligencije (AI), interneta stvari (IoT) i blockchain tehnologije predstavlja značajan korak u unapređenju digitalne sigurnosti u financijskom sektoru. AI omogućava analizu velikih količina podataka u stvarnom vremenu, detekciju prijetnji, automatizaciju sigurnosnih reakcija te predviđanje mogućih rizika na temelju povijesnih podataka, čime se unapređuje proaktivna sigurnost. IoT donosi podatke iz stvarnog svijeta u digitalne procese, omogućujući praćenje mrežnih aktivnosti, bržu reakciju na anomalije i personalizaciju usluga kroz interakciju s pametnim uređajima. Blockchain osigurava nepovredivost podataka putem decentraliziranih registara, pružajući transparentnost, sigurnost transakcija i otpornost na hakerske napade. Pametni ugovori dodatno automatiziraju procese, smanjujući rizik od prijevara i ljudskih pogrešaka. Unatoč trenutnim izazovima, kao što su sigurnosne ranjivosti, kompleksnost implementacije i relativno mali broj objavljenih radova o sinergiji ovih tehnologija, njihova integracija otvara mogućnost stvaranja naprednih sigurnosnih sustava. Ova kombinacija ne samo da jača otpornost na prijetnje, već i unapređuje povjerenje korisnika i klijenata. Rad može korisno poslužiti kao polazna točka za buduća istraživanja koja će dodatno rasvijetliti mogućnosti i izazove integracije AI-a, IoT-a i blockchaina u financijskom sektoru. Predviđa se da će zanimanje za ovu temu rasti u narednim godinama, kako se ove tehnologije budu razvijale i primjenjivale na širem globalnom nivou.

Ključne riječi: umjetna inteligencija (AI), internet stvari (IoT), blockchain, digitalna sigurnost, financijski sektor

1. Uvod

1.1. Opći uvod u temu

Digitalna transformacija omogućila je bržu i efikasniju razmjenu informacija, ali je također otvorila vrata novim prijetnjama i rizicima. U globalno

povezanom digitaliziranom svijetu, digitalna sigurnost postala je ključni aspekt za zaštitu podataka, resursa i privatnosti. Stoga je postala imperativ za sve tipove organizacija, od malih i srednjih poslovnih organizacija/poduzeća (MSP) do velikih korporacija, banaka i državnih financijskih institucija.

Razina zaštite uvelike ovisi o veličini, važnosti i razini znanja onoga tko se treba zaštititi. Velike

tvrtke mogu si priuštiti složene sigurnosne infrastrukture i timove stručnjaka, dok MSP raspolazu manjim resursima i ne mogu investirati u napredne sigurnosne sustave (Čekerevac i Bogavac, 2022). Ta disproporcija čini MSP ranjivijima na kibernetičke napade, što može imati značajne ekonomske i reputacijske posljedice. MSP se često oslanjaju na osnovne mjere zaštite koje su nedovoljne protiv sofisticiranih napada (Bogavac, 2019). Banke i državne financijske institucije su među najprivlačnijim metama za kibernetičke kriminalce zbog količine i vrijednosti podataka i financijskih sredstava kojima raspolažu. Ti entiteti moraju održavati visoke standarde sigurnosti kako bi se izborili sa sve sofisticiranijim prijetnjama, uključujući phishing napade, ransomware i napade na mrežnu infrastrukturu. Uspješna implementacija digitalne sigurnosti u bankarskom sektoru od ključne je važnosti za očuvanje povjerenja klijenata i stabilnost financijskog sustava.

Razina digitalizacije varira širom svijeta, što također utječe na sposobnost različitih regija efikasno se boriti protiv kibernetičkih prijetnji. Dok razvijene države imaju napredne digitalne infrastrukture i sofisticirane sigurnosne protokole, mnoge države u razvoju suočavaju se s osnovnim problemima digitalizacije, uključujući pristup Internetu i osnovnu kibernetičku sigurnost. (Bogavac, 2019) Ta razlika u neravnomjernosti razina zaštite, omogućava prelijevanje rizika iz regije u regiju, te povećava ranjivosti na globalnoj razini.

1.2. Cilj

Cilj ovog rada je predstaviti mogućnosti AI, IoT i blockchain tehnologija te njihove sinergijske efekte koji mogu poboljšati digitalnu sigurnost kroz efikasnije otkrivanje prijetnji, sigurno skladištenje podataka i bolju zaštitu mrežnih aktivnosti. Ove tehnologije predstavljaju budućnost digitalne sigurnosti i mogu transformirati borbu protiv cyber prijetnji.

Članak analizira koristi kao što su poboljšana proaktivna sigurnost i smanjeni rizici, te izazove povezane s implementacijom ovih tehnologija. Pregledom postojećih istraživanja i novih saznanja, članak doprinosi razumijevanju kako integracija tih tehnologija može unaprijediti digitalnu sigurnost u financijskom sektoru.

1.3. Istraživačko pitanje i hipoteze

Pristupajući istraživanju, autori su definirali istraživačko pitanje i odgovarajuće hipoteze, čime su postavljeni temelji za strukturiran i akademski pristup istraživanju te osigurana osnova za analizu.

Istraživačko pitanje: Trebaju li umjetna inteligencija, internet stvari i blockchain tehnologija biti integrirani u financijski sektor, koje koristi takva integracija može donijeti, te koje su potencijalne prijetnje povezane s ovim procesom?

Nulta hipoteza (H0): Integracija umjetne inteligencije, interneta stvari i blockchain tehnologije u financijskom sektoru ne donosi prednosti u osiguravanju otpornosti na sigurnosne prijetnje.

Alternativna hipoteza (Ha): Integracija umjetne inteligencije, interneta stvari i blockchain tehnologije u financijskom sektoru unapređuje otpornost na sigurnosne prijetnje.

1.4. Metodologija

Pri izradi ovog preglednog rada korištene su istraživačke metode koje obuhvaćaju pretragu, selekciju, analizu i sintezu relevantne literature. Literatura je pretražena u akademskim izvorima kao što su Google Scholar, IEEE Xplore, SpringerLink, MDPI i KOBSON te na relevantnim web-stranicama koje se bave zaštitom informacijskih sustava. Pretraga je uključivala i vlastite ranije objavljene radove autora, koji se bave temama iz područja IoT-a, blockchain tehnologije i digitalne sigurnosti.

U pretragu su bili uključeni i AI alati Copilot, DeepSeek i ChatGPT. Zadane su lokacije na kojima treba istražiti dostupnu literaturu i korištene su ključne riječi poput: umjetna inteligencija (AI), IoT sigurnost, blockchain, digitalna sigurnost, financijski sektor, kvantna kriptografija i kritička evaluacija. Dominantna literatura analizirana u radu bila je na engleskom jeziku, no korištena je i literatura na drugim jezicima radi obuhvatnijeg pregleda.

Pri pregledu literature izvršena je selekcija, a odabrani radovi uključeni su na temelju:

- Relevantnosti za temu (istraživanje digitalne sigurnosti u kontekstu AI-a, IoT-a i blockchaina).

- Kvalitete izvora (recenzirani radovi s pouzdanim podatkovnim osnovama).
- Datuma objave (radovi objavljeni u posljednjih pet godina, uz nekoliko relevantnih izuzetaka).

Ukupno je pretraženo 106 radova, od kojih je nakon primjene kriterija uključivanja i isključivanja za daljnju analizu odabrano 79 radova, a citirano 70 radova.

Proces evaluacije literature proveden je kroz kritičku analizu izvora, uzimajući u obzir pouzdanost podataka, metodološku valjanost i značaj nalaza za istraživačku temu.

Prikupljene informacije organizirane su tematskom analizom, pri čemu su identificirane ključne teme i obrasci koji objedinjuju dosadašnja saznanja. Tematska analiza omogućila je stvaranje konceptualnog okvira koji se fokusira na:

- Tehnološke inovacije u digitalnoj sigurnosti.
- AI, IoT i blockchain tehnologiju i digitalnu sigurnost.
- Sinergiju AI-a, IoT-a i blockchaina i
- Primjere integracije AI, IoT i blockchaina

Na temelju analize, kreirani su zaključci.

2. Tehnološke inovacije u digitalnoj sigurnosti

Tehnološke inovacije igraju ključnu ulogu u zaštiti podataka i sustava u današnjem digitalnom svijetu. Iako su inovacije nužne, nisu svima jednako dostupne, a veće organizacije često brže usvajaju nove tehnologije kako bi povećale sigurnost i nadmašile potencijalne napadače. Među najvažnijim inovacijama su:

- Umjetna inteligencija (AI) i strojno učenje (ML) za analizu podataka i otkrivanje prijetnji. Napredak u AI i ML omogućava automatizaciju složenih procesa, pružajući brzu i prilagodljivu reakciju na prijetnje. Međutim, izazovi uključuju privatnost podataka i odgovornost algoritama. Tradicionalni alati nisu dovoljni za zaštitu od novih cyber prijetnji, pa je prijelaz na

inteligentnije sustave nužan. Holistički pristup, koji uključuje suradnju stručnjaka, osigurava etičku i odgovornu primjenu ovih tehnologija (Mohamed, 2023).

- Blockchain, decentralizirana tehnologija koja omogućuje sigurno i nepromjenjivo bilježenje transakcija u distribuiranom lancu blokova. Svaki blok sadrži transakcije koje su kriptografski povezane. Sigurnost se postiže konsenzusnim mehanizmima, čime se eliminira potreba za centralnim autoritetom i smanjuje rizik od prijevare i manipulacije (Cekerevac i Cekerevac, 2022). Sadašnja razina razvoja ove tehnologije omogućuje njenu uspješnu primjenu i u velikim, ali i u MSP (Cekerevac i Cekerevac, 2023).
- Napredni kriptografski algoritmi za zaštitu podataka, uključujući kvantnu kriptografiju, homomorfno šifriranje, kao i njihovu kombinaciju, kvantno homomorfno šifriranje (QHE). Kvantna kriptografija koristi principe kvantne mehanike za osiguranje sigurne komunikacije. Najpoznatija primjena kvantne kriptografije je kvantna distribucija ključeva (QKD), koja omogućava bezuvjetno sigurnu razmjenu tajnih ključeva između dvije strane koristeći kvantne fenomene (Jaćimovski i sur. 2019). Homomorfno šifriranje omogućava izvođenje operacija na šifriranim podacima bez njihovog dešifriranja, čime se osiguravaju privatnost i sigurnost podataka tokom obrade (IBM, What is homomorphic encryption?, 2024). QHE omogućava izvođenje kvantnih operacija na šifriranim kvantnim podacima (kubiti) bez njihovog dešifriranja (Yarter i sur., 2022). Ove tehnologije predstavljaju značajan napredak u sigurnosti podataka, omogućujući zaštitu informacija čak i tijekom obrade. Homomorfno šifriranje je već u praksi, dok kvantno homomorfno šifriranje ima potencijal za revolucioniranje načina na koji će se obavljati računske operacije u budućnosti.
- Tehnologije kibernetičke obmane koje obuhvaćaju mjere koje omogućuju upućivanje napadača na lažne resurse i skreću napade na prave ciljeve. To omogućuje rano otkrivanje prijetnji, proaktivno djelovanje i poboljšanje odgovora na napade (EclipseForensics, 2024).

- Biometrijska autentifikacija koristi fizičke karakteristike za verifikaciju identiteta i danas je udomaćena na mobilnim uređajima i na stacionarnim uređajima kod kojih se zahtjeva visoka razina zaštite. Sofisticiranija je bihevioralna biometrija koja analizira jedinstveno ponašanje korisnika, kao što su obrasci tipkanja, pokreti mišem i čak geste na dodirnom ekranu (Finnegan i sur. 2024). Ove karakteristike dodaju dodatni sloj sigurnosti, poboljšavajući sustave višefaktorske autentifikacije.
- Zero Trust, arhitektura koja zahtijeva verifikaciju svakog korisnika i uređaja pri svakom pristupu sustavu (Levin, 2024). Napredak u alatima koji pojednostavljaju implementaciju Zero Trusta učinili su ovu tehnologiju jednostavnijom za primjenu.
- Sigurnost IoT uređaja primjenom laganih protokola šifriranja i autentifikacije. Ovi protokoli su posebno dizajnirani za uređaje s ograničenom procesorskom snagom i koriste implicitne certifikate za pružanje međusobne autentifikacije i dogovora o ključu između IoT uređaja (Siddharta i sur. 2020).
- Sigurni pristup na rubu mreže (SASE) je integrirana mrežna i sigurnosna arhitektura koja spaja funkcije mrežnog povezivanja i sigurnosti kroz distribuiranu cloud infrastrukturu. SASE omogućuje siguran pristup resursima i aplikacijama bez obzira na lokaciju korisnika. Dizajniran je da pruži efikasan, skalabilan i siguran pristup resursima, omogućujući organizacijama lakše suočavanje sa sve složenijim sigurnosnim prijetnjama (Cisco, 2024).
- Upravljanje identitetima i pristupom (IAM) podrazumijeva skup politika, procesa i tehnologija koji se koriste za upravljanje digitalnim identitetima korisnika i kontrolu pristupa resursima unutar organizacije. Cilj IAM-a je osigurati da su pravi korisnici u pravom trenutku ovlašteni za pristup pravim resursima, uz kontinuirano praćenje i prilagođavanje prava pristupa. IAM obuhvaća i novije pristupe poput Self-Sovereign Identity (SSI), koje omogućuju korisnicima veću kontrolu nad vlastitim digitalnim identitetima (Glöckler i sur. 2024). Posebna pažnja posvećuje

se sigurnosti u oblaku, koja omogućuje centralizirano definiranje i provođenje sigurnosnih politika, uz decentralizirano upravljanje pristupom podacima (Alsirhani i sur. 2022).

- Zaštita na razini podatka (DLP) prati, detektira i kontrolira osjetljive podatke kako bi se spriječio neovlašteni pristup, gubitak ili krađa. Implementira pravila i politike za zaštitu podataka u tranzitu, pohrani i upotrebi, osiguravajući usklađenost s regulativama i sigurnost informacija (Vaideeswaran, 2025).

Inovacije naglašavaju pomak ka proaktivnijim sigurnosnim mjerama, predviđajući ponašanje napadača. Težnja je automatizirati procese zaštite. Homomorfno šifriranje i kvantno-otporna kriptografija rješavaju dugoročne sigurnosne izazove. Pri ovome se podrazumijevaju primjena AI-a u zaštiti, suradnja u osiguranju samih AI sustava i dijeljenje informacija o prijetnjama. Okviri za osiguranje AI-a i dijeljenje informacija o prijetnjama ističu važnost suradnje i predviđanja u obrani protiv sve složenijih prijetnji. Svaka od ovih inovacija donosi izazove u pogledu pouzdanosti i otpornosti na napade, a potrebni su resursi i vrijeme za kompletne provjere.

3. AI, IoT i blockchain tehnologija i digitalna sigurnost

3.1. Umjetna inteligencija (AI)

Umjetna inteligencija (AI) je ključna tehnologija koja omogućava računalima obavljanje zadataka koji inače zahtijevaju ljudsku inteligenciju. Igra važnu ulogu u poboljšanju digitalne sigurnosti, posebno u bankama i državnim institucijama, ali i za zlonamjerne napadače. Korištenjem algoritama strojnog učenja, AI sustavi mogu analizirati velike količine podataka u stvarnom vremenu i otkriti prijetnje i anomalije. Glavni pozitivni utjecaji AI na sigurnost uključuju:

- Detekciju prijetnji (Skoromets, 2024): Mnoge banke koriste AI za detekciju i prevenciju prijevara u stvarnom vremenu. AI algoritmi analiziraju transakcije i ponašanje korisnika kako bi identificirali neuobičajene aktivnosti

(poput neovlaštenih transakcija ili pokušaja krađe identiteta) i spriječili potencijalnu štetu. Analizom podataka i identifikacijom sumnjivih aktivnosti, AI pomaže u otkrivanju i blokiranju zlonamjernog softvera. Također, AI podržava digitalne asistente u online bankarstvu koji klijentima nude sigurnije i personaliziranije usluge.

- Upravljanje identitetima: AI omogućava precizno upravljanje identitetima i kontrolom pristupa osjetljivim informacijama.
- Automatizaciju sigurnosnih provjera: Automatizacija sigurnosti podrazumijeva odgovor na cyber prijetnje uz minimalnu ili nikakvu ljudsku intervenciju. Alati za automatizaciju detektiraju prijetnje, klasificiraju incidente i odlučuju o mjerama za ublažavanje prijetnji, osiguravajući skalabilno i učinkovito upravljanje sigurnošću. Umjetna inteligencija omogućuje značajno poboljšanje sigurnosnih sustava automatizacijom zadataka. Ova tehnologija osigurava agilniji pristup zaštiti podataka i sustava, pa je zato pogodna za “zero trust” sigurnosni koncept osmišljen za suočavanje s rastućim brojem i složenošću cyber prijetnji. AI se fokusira na preciznu kontrolu pristupa temeljenu na RBAC (kontrola pristupa prema ulozi), eliminirajući implicitno povjerenje unutar mreže. Zbog zahtjevnosti ovakve granularne sigurnosti, automatizacija sigurnosnih procesa je ključan element zaštite. Pored toga, automatizacija smanjuje opterećenje sigurnosnih timova automatizirajući rutinske zadatke, čime omogućuje brže reagiranje

na prijetnje i povećanje učinkovitosti. Također, automatizacija smanjuje rizik od ljudskih grešaka i osigurava usklađenost s regulativama. Jedan od značajnih razloga za uvođenje automatizacije u zaštitu je usuglašavanje sa propisima o cyber sigurnosti i industrijskim standardima. Upravljanje sigurnosnim zahtjevima i pojedinačnim certifikatima je složen proces, posebno imajući u vidu promjene u industriji i zakonskim zahtjevima. Automatizacija olakšava održavanje razine usklađenosti i certifikacije (Tubin, 2024).

No, AI također donosi rizike:

- Zlonamjerni napadači mogu koristiti AI za sofisticirane napade, poput phishing kampanja i deepfake tehnologije.
- Privatnost i sigurnost podataka: Analiza podataka putem AI može ugroziti privatnost ako se ne koriste odgovarajuće mjere zaštite.
- Etička pitanja: Transparentnost i odgovornost u donošenju odluka zasnovanih na AI također su važna.

Umjetna inteligencija može značajno poboljšati digitalnu sigurnost, ali također predstavlja nove rizike koji zahtijevaju pažljivo upravljanje i stalno poboljšanje obrambenih strategija. Stoga je važno razmotriti sve potencijalne scenarije primjene AI. Tablicom 1. sažeto je prikazana zastupljenost umjetne inteligencije u digitalnoj sigurnosti.

Tablica 1. Zastupljenost AI u digitalnoj sigurnosti

Tip AI u digitalnoj sigurnosti	Cilj	Primjeri
Obrambena AI	Korištenje AI tehnika za zaštitu računalnih sustava i mreža od napada	Anti-malware; Sustavi za detekciju upada (IDS)
Ofenzivna AI	Primjena AI tehnika za napad na računalne sustave i mreže	Razvoj novih cyber napada; Automatizacija iskorištavanja postojećih ranjivosti
Adversarialna AI	Zlonamjerno iskorištavanje i/ili napadanje AI/ML sustava i podataka	Trovanje podataka za obuku; Manipulacija ulaznim podacima

Izvor: Malatji i Tolah (2024).

Analize ofenzivnih AI cyber napada otkrivaju njihovu složenu i dinamičnu prirodu. Zbog toga su potrebni adaptivni obrambeni mehanizmi podržani umjetnom inteligencijom. Svaki napad vođen AI-om je višedimenzionalan i uključuje razne implikacije, strategije, motivacije i društvene utjecaje. To otežava zaštitu i naglašava potrebu za sofisticiranijim metodama obrane. (Sajid, 2024; Darktrace, 2021).

U vezi sa AI mora se naglasiti potreba ne samo za korisnim AI sustavima, već i otpornim na cyber napade. U tom pogledu pomažu tehnike kao što su "adversarial training". One pomažu AI sustavima braniti se od manipulacija, kao što su napadi koji pokušavaju prevariti algoritme strojnog učenja (Zhao i sur. 2022; Soundenkar i sur. 2024). Ovo je posebno važno, jer financijski sustavi moraju biti neprekidno sigurni, čak i protiv sofisticiranih prijetnji.

Kako AI postaje ključna tehnologija, zakonodavci i regulatori igraju važnu ulogu u osiguravanju sigurnog i etičkog korištenja. U financijskom sektoru, regulacije poput GDPR (Opća uredba EU o zaštiti podataka) (2024) u EU štite podatke korisnika, dok propisi potiču transparentnost u primjeni AI modela.

Uvođenje umjetne inteligencije realno zahtijeva suradnju između banaka, tehnoloških tvrtki i regulatora. Banke mogu surađivati s tehnološkim inovatorima na razvoju AI rješenja za sprječavanje prijevара, dok regulatori osiguravaju da su ta rješenja u skladu s pravnim okvirom. Takva sinergija je ključna za brži napredak i širu AI primjenu.

3.2. Internet stvari (IoT) i njegov utjecaj na financijsko poslovanje

Internet stvari (IoT) postaje sve značajniji u ekonomiji jer omogućava prikupljanje i razmjenu podataka u stvarnom vremenu, što je ključno za financijske transakcije. Pomaže u analizi imovine klijenata i digitalizaciji operacija financijskih kompanija, poboljšavajući usluge i korisničko iskustvo. IoT podržava prijenos podataka preko različitih uređaja povezanih putem Bluetootha, WiFi-a ili USB-a te omogućava praćenje mrežnih aktivnosti i detekciju prijetnji, čime poboljšava digitalnu sigurnost. Sigurnost IoT uređaja je od ključne važnosti zbog njihove povezanosti s mrežom i nedovoljno sigurnih protokola, što ih čini lakšom metom

napada (Kumar i sur. 2023; Alliou i Mourdi, 2023; Yilmaz i Hazar, 2019).

Globalno tržište IoT-a u sektoru bankarsko-financijskih i usluga osiguranja (BFSI) dostiglo je 2.030 milijuna dolara do 2023. godine, što je porast sa 249,4 milijuna dolara u 2018. godini, uz godišnji rast od 52,1% (techblog, 2022).

3.2.1. Kako IoT utiče na financijsko poslovanje?

Internet stvari (IoT) ima brojne primjene u financijskom poslovanju koje mogu poboljšati učinkovitost, sigurnost i kvalitetu usluga. IoT omogućava prikupljanje podataka u realnom vremenu, olakšavajući analizu i donošenje odluka. Primjerice, klijenti mogu biti odmah obaviješteni o neuobičajenim troškovima, a pametni uređaji mogu pratiti redove u poslovnicaма i omogućiti zakazivanje posjeta. IoT također poboljšava sigurnost otkrivanjem neuobičajenog ponašanja u realnom vremenu, kontroliranjem pristupa računima i korištenjem biometrijske autentifikacije. Među najznačajnijim doprinosima IoT uređaja nalazi se podrška za automatizaciju procesa, poput otvaranja računa i obrade zahtjeva, što može smanjiti troškove i povećati učinkovitost.

IoT omogućava financijskim institucijama bolje razumijevanje potreba klijenata i pružanje personaliziranih usluga. Uređaji prikupljaju podatke koji unapređuju financijske usluge tijekom cijelog ciklusa, dok analitika podataka pomaže u upravljanju novcem klijenata. Također omogućava praćenje imovine u realnom vremenu, optimizirajući upravljanje i smanjujući troškove. IoT podržava bolje praćenje i analizu tržišnih podataka te upravljanje zalihama. Omogućava bežične uplate putem uređaja poput pametnih satova i telefona, pružajući korisnicima pristup sredstvima bilo gdje i bilo kada (Nilay, 2024).

3.2.2. Primjeri primjene IoT u financijskom poslovanju

Financijska tehnologija (fintech), koristi nove tehnologije za unapređenje i automatizaciju financijskih usluga, omogućavajući brže, učinkovitije i sigurnije transakcije. Bankarstvo već desetljećima koristi koncept interneta stvari (IoT). Neki primjeri primjene IoT-a u financijskom poslovanju

uključuju pametne bankomate, bežična plaćanja putem pametnih telefona i satova te mobilne POS (*Point-of-Sale*) sustave.

Manje uočljive, ali značajne primjene IoT-a uključuju pametne uređaje za praćenje financijskog stanja korisnika, pametne bankarske strojeve za dodatne sigurnosne mjere, pametne alarme za sigurnost, te senzore za praćenje inventara, npr. u trezorima, skladištima i prodavaonicama (Čekerevac i sur. 2010). IoT tehnologija je revolucionirala financijsko poslovanje omogućavajući brže, sigurnije i personalizirane usluge klijentima (Nilay, 2024; techblog, 2022).

Fintech također koristi nove tehnologije za unapređenje financijskih usluga kao što su mobilno bankarstvo, P2P pozajmljivanje, kriptovalute, robo-savjetnici, digitalni novčanici. Fintech transformira način poslovanja s financijama, čineći ih pristupačnijima, transparentnijima i učinkovitijima (Bwalya i Paul, 2024; Suresh i Manoj. Nove tehnologije se koriste i u osiguranju (InsurTech) za poboljšanje procesa osiguranja. Najznačajniji primjeri uporabe IoT za ove namjene su preciznija procjena rizika, automatizacija obrade šteta, preventivne mjere i poboljšanje korisničkog iskustva. U tu svrhu, IoT uređaji, poput smart home uređaja, pametnih satova, GPS uređaja i senzora u vozilima, i uopće smart uređaja, omogućuju prikupljanje podataka u stvarnom vremenu. Osiguravatelji mogu koristiti ove podatke za precizniju procjenu rizika i prilagodbu premija na temelju stvarnog ponašanja korisnika. IoT senzori mogu automatski prijaviti nesreće ili štete, pružajući osigurateljima detaljne informacije o incidentu. To ubrzava proces obrade zahtjeva i smanjuje mogućnost prijevара. (Dallinger, 2024; Behm i sur., 2019). Pametni uređaji, poput detektora dima ili senzora za curenje vode, mogu ukazati na potencijalne probleme prije nastanka većih šteta.

3.2.3. Može li IoT biti žrtva napada?

Elektronski podaci su česta meta napada, osobito kada su povezani s Internetom (Čekerevac i sur. 2018). IoT uređaji, uključujući one u financijskom sektoru, izloženi su napadima koji se mogu prenijeti i na pripadajuće blockchain sustave. Primjerice, napadači mogu iskoristiti slabosti u lozinkama ili ugrađenom programskom softveru kako bi neovlašteno pristupili uređajima, dok tzv.

Man-in-the-Middle (MITM) napadi omogućuju prešretanje komunikacije i manipulaciju podacima (Čekerevac i sur. 2017). Također, usluge se mogu ometati preplavlivanjem zahtjevima u *Denial of Service* napadima, a uređaji mogu postati ranjivi ako njihov ugrađeni programski softver nije adekvatno održavan.

Osim toga, fizički pristup uređajima napadačima omogućuje ugrađivanje zlonamjernog koda, dok su šifrirani podaci u opasnosti ako napadači steknu pristup ključevima za šifriranje. Slabosti u lozinkama, poput korištenja zadanih postavki, također mogu dovesti do neovlaštenog pristupa, a sofisticirani napadi, poput Side-Channel tehnika, iskorištavaju potrošnju energije ili zvuk za dobivanje povjerljivih informacija. *"Brute force"* metode dodatno ugrožavaju sigurnost pokušajima probijanja lozinki, dok ranjivosti u softverskim ažuriranjima omogućuju neovlaštenu kontrolu nad uređajima (Coston i sur. 2025; Madiarbekova, 2025; Devi i Majumder, 2020).

Glavni razlozi za ranjivost IoT uređaja leže u tome što mnogi IoT uređaji zbog ograničenih resursa mogu poduzimati samo minimalne sigurnosne mjere zaštite, što proizvođači rijetko pružaju redovita sigurnosna ažuriranja, a i kada ih pružaju, korisnici ih često ne koriste. Slabe lozinke ili nedostatak autentifikacije omogućuju neovlašten pristup, pa napadači mogu preuzeti kontrolu i koristiti uređaje za distribuirano uskraćivanje usluge (DDoS).

Stvarni i potencijalni napadi na IoT ističu potrebu za stalnim usavršavanjem obrambenih strategija kako bi se zaštitili financijski IoT uređaji i mreže, te očuvala njihova sigurnost.

3.3. Blockchain tehnologija

Koncept korištenja nematerijalne imovine, poput licenci, žigova, patenata i kriptovaluta, dobro je poznat u financijskom sektoru. Blockchain tehnologija, najčešće povezivana s Bitcoinom, omogućava decentraliziranu i transparentnu zaštitu podataka, čuvajući njihovu autentičnost i nepovredivost. Idealan je alat za sigurno skladištenje i provjeru transakcija, smanjujući rizik od manipulacija i prijevара (Čekerevac i sur. 2018).

Blockchain omogućava financijske transakcije bez vremenskih ograničenja i neovisno o bankama ili državama. Blockchain se neće detaljno opisivati,

ali treba pomenuti da se temelji na tri tehnologije: kriptografiji s privatnim ključem, P2P mreži i protokolu koji upravlja poticajima. Svaki od korisnika u distribuiranoj mreži ima kopiju glavne knjige što sprječava mogući gubitak podataka i jedinstvenu točku kvara (SPOF). Sve kopije transakcija se ažuriraju i provjeravaju u isto vrijeme. Glavna knjiga lanca blokova sadrži kronološki zapis svake transakcije u obliku lančano povezanih kriptografski provjerljivih dijelova (Čekerevac i sur. 2018). Stalna tehnološka poboljšanja ubrzavaju procese i stabiliziraju vrijednost kriptovaluta. Osim što smanjuje transakcijske troškove eliminiranjem posrednika, blockchain je otporan na mnoge vrste napada, uključujući i MITM napade.

Međutim, IoT uređaji povezani s blockchainom predstavljaju potencijalnu slabost ukoliko nisu pravilno zaštićeni, što može ugroziti integritet podataka i sigurnost sustava. Kompromitirani IoT uređaji mogu slati netočne podatke na blockchain, manipulirati pametnim ugovorima ili izazvati preopterećenje mreže kroz distribuirane DDoS napade. Također, krađa identiteta i ransomware napadi mogu dovesti do ozbiljnih sigurnosnih problema. Zbog toga je nužno provesti sigurnosne mjere kao što su osiguranje komunikacije prije nego podaci stignu na blockchain, snažno šifriranje i autentifikacija uređaja, implementacija sigurnih protokola za pokretanje uređaja te redovita ažuriranja softvera. Pravilna identifikacija IoT uređaja i kontinuirano praćenje njihovih sigurnosnih postavki pomaže u smanjenju rizika i očuvanju sigurnosti blockchain mreže.

Primjena ovih mjera, uključujući inicijalne i periodične provjere, kriptografske verifikacije transakcija i pametne ugovore, osigurava pouzdanost IoT uređaja i blockchain sustava te smanjuje prijetnje kojima su izloženi.

Primjena blockchain tehnologije povezana je i s problemima kao što su interoperabilnost, skalabilnost i upotrebljivost, koji mogu uzrokovati uska grla te se pojavila ideja da se formira mreža međusobno povezanih blockchain mreža, odnosno *"blockchain of blockchains"*. Ovaj koncept omogućava različitim blockchainovima međusobno komunicirati i dijeliti podatke, čime se povećavaju interoperabilnost i učinkovitost. Ideja postoji, na njoj se radi, ali nije dostigla razinu industrijskog standarda. Neki od aktualnih projekata su Polkadot i Cosmos (Puah, 2022).

4. Integracija AI, blockchain i IoT radi poboljšanja digitalne sigurnosti

Većina dosadašnjih studija bavila se integracijom IoT-a i AI-a ili IoT-a i blockchaina (Alharbi i sur. 2022). Razvoj umjetne inteligencije omogućava integraciju sve tri tehnologije, osiguravajući sigurnost IoT mreže. Za očekivati je da integracija umjetne inteligencije (AI), blockchain-a i Internet of Things (IoT) može značajno doprinijeti poboljšanju digitalne sigurnosti, posebno u kontekstu zaštite financijskih sustava i procesa.

Som i Kayal (2022) su zaključili da integracija umjetne inteligencije (AI), blockchaina i Interneta stvari (IoT) predstavlja temelje za transformaciju financijskog sektora. IoT omogućuje prikupljanje podataka u stvarnom vremenu, blockchain pruža decentraliziranu i sigurnu infrastrukturu, dok AI optimizira procese i analizira podatke. Ova kombinacija otvara prilike za stvaranje autonomnih poslovnih modela i novih izvora prihoda putem pametnih ugovora i tokenizacije IoT uređaja, čime se povećavaju konkurentnost i digitalna sigurnost. FinTech dodatno revolucionira financijske usluge kroz inovacije poput digitalnih novčanika i blockchain tehnologije, pružajući učinkovitije i transparentnije alternative tradicionalnim procesima. Međutim, izazovi poput sigurnosnih prijetnji i potrebe za značajnim ulaganjima i dalje otežavaju punu implementaciju ovih tehnologija. Ove tehnologije zajedno stvaraju temelje za decentralizirane, sigurnije i učinkovitije sustave, čime omogućuju digitalnu transformaciju koja će oblikovati budućnost financijskog sektora.

Zaključak studije Alharbi i sur. (2022) naglašava integraciju umjetne inteligencije (AI), blockchaina i Interneta stvari (IoT) kao obećavajući pristup za unapređenje sigurnosti IoT mreža. Analizirane su arhitekture IoT-a, sigurnosni zahtjevi, izazovi i ranjivosti, zajedno s karakteristikama i vrstama blockchain tehnologije. Na temelju istraživanja provedenog u razdoblju od 2017. do 2022., evidentan je rast interesa za ovu tehniku. Studija identificira tri klase rješenja: temeljena na AI, temeljena na blockchainu i ona koja integriraju obje tehnologije. Većina postojećih radova fokusira se na povezivanje IoT-a s jednom od ovih tehnologija, što ističe potrebu za njihovom zajedničkom

integracijom radi zaštite mreža. Studija identificira praznine u istraživanju, posebno u razvijanju distribuiranih modela obrane koji istovremeno osiguravaju privatnost. Integracija AI-a i blockchaina s IoT-om može rezultirati decentraliziranim sustavima, sigurnom razmjenom podataka i transakcijama te nepovredivim IoT mrežama. Ovo istraživanje predlaže buduće smjerove, uključujući reviziju distribuiranih IDS modela i izgradnju suradničkog sustava za ublažavanje napada. Tehnologija je u ranoj fazi razvoja i zahtijeva daljnja istraživanja.

Rane i sur. (2023) su zaključili da kombinacija blockchain tehnologije i umjetne inteligencije (AI) unosi transformativne promjene u financijski sektor, poboljšavajući sigurnost, transparentnost i učinkovitost. Blockchain, kao decentralizirani i nepovredivi zapisnik, omogućuje trajno čuvanje podataka, čime štiti od cyber prijetnji i prijevara. AI doprinosi prediktivnom analizom, strojnim učenjem i automatizacijom, omogućujući analizu podataka u stvarnom vremenu, procjenu rizika i optimizaciju procesa. Njihova zajednička primjena povećava točnost financijskih podataka i osigurava sigurnost kroz automatizirane procese poput "Know Your Customer (KYC)" i "Anti-Money Laundering (AML)". Blockchain omogućuje sigurnu pohranu korisničkih podataka, dok AI prepoznaje sumnjive aktivnosti u velikim bazama podataka, pridonoseći usklađenosti s regulativama. Pametni ugovori automatiziraju sporazume, smanjujući greške i troškove, dok AI dodatno prilagođava njihove funkcije. Transparentnost koju blockchain donosi jača povjerenje među sudionicima financijskih transakcija, a AI poboljšava detekciju prijevara i upravljanje rizicima. Integracija ovih tehnologija predstavlja revoluciju koja otvara nove mogućnosti za razvoj inovativnih i učinkovitih financijskih ekosustava.

Zalhusni (2024) također analizira mogući utjecaj blockchaina, IoT i AI na digitalnu transformaciju i zaključuje da napredak ovih tehnologija stvara povezan ekosustav koji transformira industrije. Blockchain pruža povjerenje kroz transparentnost i pametne ugovore, IoT generira podatke, dok AI koristi te podatke za optimizaciju procesa i stvaranje autonomnih uređaja. Digitalni novčanici, podržani blockchainom, integriraju tokenizirane depozite, povezujući tradicionalno bankarstvo s modernim tehnologijama. IoT uređaji mogu autonomno upravljati transakcijama, poput plaćanja

pri punjenju električnih vozila (EV), čime doprinose razvoju održivijih financijskih modela. Decentralizirane infrastrukturne mreže omogućuju zajedničama zajedničko upravljanje resursima, dok vlade istražuju blockchain kroz digitalne valute centralnih banaka (CBDC), integrirajući ga u financijske politike. Kombinacija ovih tehnologija obećava transformaciju industrija i stvaranje digitalnog ekosustava do 2030. godine (Zulhusni, 2024).

Chilamkurti i sur. (2024) razmatraju integraciju temeljnih koncepata blockchaina, IoT-a i umjetne inteligencije (AI), pružaju detaljan pregled tehnoloških izazova i mogućnosti u ovim područjima te istražuju kako njihova kombinacija redefinira poslovanje. Fokusiraju na stvarne primjere i aplikacije, ističući kako blockchain omogućuje povjerenje, transparentnost, pametne ugovore i automatizaciju. IoT može generirati podatke iz milijardi uređaja, dok AI pruža analitičke alate za optimizaciju procesa. Naglašavaju se brzina i stabilnost blockchaina, čime se olakšava stvaranje inteligentnih sustava i okruženja. Spomeniti autori objašnjavaju kako blockchain može povećati točnost i integritet IoT podataka te ističu korištenje pametnih ugovora i distribuiranih knjiga.

Nofel i sur. (2024) su predstavili sustavni pregled literature o integraciji blockchaina, IoT-a i XBRL tehnologija unutar sustava za računovodstvene informacije (AIS). Analizirali su 309 istraživanja u razdoblju od 2013. do 2023., pri čemu je identificirana važnost ove tehnološke konvergencije za unapređenje transparentnosti, izvještavanja u stvarnom vremenu i sigurnosti podataka. Blockchain, decentralizirana i nepovrediva tehnologija zapisnika, može transformirati tradicionalno računovodstvo kroz trojni računovodstveni sustav, povećavajući transparentnost i smanjujući slučajeve prijevara. IoT omogućuje prikupljanje podataka u stvarnom vremenu i automatizaciju, dok XBRL donosi standardizaciju i usporedivost financijskih podataka za lakšu analizu i objavljivanje informacija. Autori su zaključili da iako ove tehnologije nude brojne koristi, njihova integracija suočava se s izazovima poput kibernetičkih prijetnji, velikih infrastrukturnih zahtjeva i nedostatka stručnjaka. Buduća istraživanja trebaju koristiti empirijske metode za testiranje praktične primjene i utjecaja integriranih sustava, uz razvoj standardiziranih protokola i najboljih praksi za smanjenje rizika i maksimizaciju koristi.

Cilj istraživanja autora Sharma i sur. (2024) bio je rasvijetliti budućnost financijskih transakcija kroz širu primjenu naprednih tehnologija, povećavajući povjerenje i učinkovitost u sve digitalnijem svijetu. I za ove autore integracija blockchaina, IoT-a i umjetne inteligencije (AI) predstavlja revolucionarnu priliku za bankarski sektor, posebno u unapređenju učinkovitosti pametnih ugovora. I po njima, ove tehnologije mogu značajno poboljšati transparentnost, sigurnost i učinkovitost financijskih transakcija: Blockchain pruža decentraliziranu i nepovredivu infrastrukturu, IoT omogućuje prikupljanje podataka u stvarnom vremenu, dok AI analizira podatke i optimizira procese. Njihova istraživanja ukazuju na sinergijske prednosti ove integracije, uključujući smanjenje prijevара, bolje upravljanje procesima i povećanje povjerenja dionika. Stvaranje odgovornijeg i transparentnijeg financijskog ekosustava zahtijeva rješavanje postojećih izazova i razvoj praktičnih rješenja za njihovu implementaciju. Integracija ima potencijal ne samo na teorijskoj razini, već i u praksi.

Iako se mali broj istraživanja do sada bavio sinergetskim djelovanjem blockchain tehnologije, AI i IoT uopće, a posebno u području financija, može se primijetiti da se u 2024. godini povećao broj objavljenih takvih radova, ali da im zaključci konvergiraju u isticanju potencijala njihovog objedinjavanja. Blockchain, IoT i AI stvaraju povezan ekosustav koji unaprjeđuje industrije kroz transparentnost, optimizaciju i autonomne procese. Blockchain pruža povjerenje, IoT generira podatke, a AI ih koristi za analizu. Digitalni novčanici i autonomna plaćanja omogućuju održive financijske modele povezivanjem tradicionalnog bankarstva s modernim tehnologijama. Ključni potencijali svakog od učesnika u integraciji su:

1. Umjetna inteligencija (AI) može analizirati velike količine podataka u stvarnom vremenu, prepoznati sumnjive obrasce ponašanja koji mogu prethoditi prijevaram ili napadu i automatski reagirati na prepoznate prijetnje, omogućavajući brže i efikasnije odgovore na incidente. Pomoću povijesnih podataka, AI modeli mogu predvidjeti moguće prijetnje i ranije upozoriti na rizike.
2. Blockchain osigurava nepromjenjive registre transakcija pri čemu su transakcije

transparentne i verificirane, čime se smanjuje mogućnost prijevara i osigurava nepovredivost podataka. Distribuiranost čini blockchain otpornim na hakiranje. Pametni samoizvršivi ugovori mogu automatski izvršavati transakcije kada su ispunjeni uvjeti, čime se smanjuje mogućnost ljudske greške i prijevara.

3. Internet stvari (IoT) omogućuje povezivanje različitih uređaja, osiguravajući da podaci iz fizičkog (analognog) svijeta budu integrirani u digitalne procese što može poboljšati efikasnost i bezbjednost transakcija. Pametni senzori mogu praćenjem aktivnosti i stanja uređaja omogućiti brzu detekciju i odgovor na sigurnosne prijetnje. IoT uređaji mogu generirati potrebne podatke koji se mogu koristiti za analizu i prepoznavanje potencijalnih prijetnji.

Kombiniranjem AI, blockchain i IoT tehnologija, organizacije mogu stvoriti robustan okvir za zaštitu svojih financijskih sustava i procesa. Ove se tehnologije međusobno nadopunjuju, omogućujući unaprjeđenje prediktivnih i reaktivnih mjera zaštite. Osim toga, ovakav sustav može povećati povjerenje među korisnicima i klijentima, čime se jača cjelokupna infrastruktura digitalne sigurnosti.

5. Primjeri integracije AI, IoT i blockchaina

Postoji niz proizvoda poznatih proizvođača koji se bave integracijom blockchaina, umjetne inteligencije (AI) i Interneta stvari (IoT). Neki nude potpuno integrirana rješenja, dok većina nudi ili integraciju dviju tehnologija ili pojedinačna rješenja koja se mogu integrirati uz primjenu dodatnih alata ili aplikacija. Neki od najpoznatijih ponuđača su:

- **IBM:** IBM Watson IoT® Platform i IBM Blockchain Platform. Prva platforma omogućuje upravljanje IoT podacima uz analizu i prilagodbu pomoću umjetne inteligencije (IBM, 2024). Također, IBM Blockchain Platform (IBM, IBM Support for Hyperledger Fabric, 2024) koristi podatke iz IoT uređaja za stvaranje sigurnih i nepovredivih zapisa transakcija.

- **Microsoft:** Azure Blockchain Service, Azure AI i Azure IoT Hub. Microsoft platforme Azure mogu surađivati kako bi stvorile rješenja za različite industrije, poput pametnih gradova, logistike i financija. Pritom Azure IoT omogućuje povezivanje i upravljanje IoT uređajima, Azure Blockchain Service pruža infrastrukturu za sigurne i decentralizirane transakcije, a Azure AI nudi alate za analizu podataka i optimizaciju procesa (Kataria, 2025; Azure, 2025; Azure, bez dat.).
- **Intel:** Intel nema specifičnu platformu koja eksplicitno objedinjuje AI, IoT i blockchain, ali nudi tehnologije i rješenja koja podržavaju ova područja. Intel pruža hardverske i softverske alate za AI kroz procesore i optimizirane algoritme, a njihova IoT rješenja omogućuju povezivanje uređaja i upravljanje podacima. Intel također podržava blockchain tehnologiju kroz procesore dizajnirane za optimizaciju rudarenja i sigurnost podataka. Integracija ovih tehnologija može se ostvariti kombiniranjem Intelovih proizvoda i platformi s dodatnim softverskim rješenjima (Intel Corporation, 2022; Intel, 2024; Intel Corporation, 2018).
- **Amazon Web Services (AWS) (2025):** Amazon Managed Blockchain, Amazon SageMaker, Amazon IoT Core i druge. Ove platforme nisu dizajnirane kao integrirana platforma koja automatski objedinjuje sve tri tehnologije, ali ih je uz pametne ugovore i AWS Lambda (AWS, 2025) usluge moguće integrirati.
- **Huawei:** Huawei za sada, ne nudi objedinjenu platformu, ali nudi komponente sustava. Kombiniranjem funkcionalnosti platforme OceanConnect IoT (Jidong i Yaqing, 2018), Huawei Cloud AI (Huawei, 2025) alata za umjetnu inteligenciju i Huawei Blockchain Service (BCS) (Xiaojun, 2025), uz dodatne prilagodbe za specifične aplikacije, može se ostvariti integracija AI, IoT i blockchaine.
- **Cisco Systems:** Cisco Kinetic for IoT (Venkatachalam i Siraj, 2019) i Cisco Blockchain (Vignette, 2019; Cisco, 2018). Cisco Kinetic for IoT fokusira se na upravljanje IoT podacima, dok Cisco Blockchain tehnologija koristi decentralizirane

registre za sigurnost i transparentnost podataka. Kombiniranjem ove dvije tehnologije kroz prilagođena rješenja, koristeći Cisco proizvode zajedno s dodatnim softverskim alatima moguće je postizanje integracije blockchaine, IoT-a i AI-a.

Postoje i rješenja manje poznatih proizvođača i startupova. Pitanje je koliko će ovakva rješenja biti uspješna na tržištu, ali su principi na kojima su rješenja kreirana inventivni i mogu nadživjeti same kompanije iz kojih potječu. Jednu grupu platformi, koja integracijom AI-a, blockchaine i kvantno-otporne sigurnosti jača digitalno povjerenje, kreirala je WISEKey. Ona uključuje (Choucair, 2025; SEALSQ, 2024):

- **WISEkey WISEID:** platforma za digitalni identitet i sigurnost. WISEID koristi umjetnu inteligenciju za analizu ponašanja i autentifikaciju, IoT za povezivanje uređaja, te blockchain za decentraliziranu infrastrukturu i zaštitu podataka (Choucair, 2025).
- **SEALSQ:** specijalizirana platforma za postkvantnu kriptografiju i sigurne digitalne identitete. Iako SEALSQ ne objedinjuje automatski AI, IoT i blockchain u jedinstvenu platformu, pruža tehnologije koje omogućuju njihovu integraciju. Postkvantni čipovi SEALSQ osiguravaju visok stupanj sigurnosti za IoT uređaje i podatke. Blockchain infrastruktura omogućuje sigurne transakcije i transparentnost podataka. AI-driven sigurnosni mehanizmi koriste umjetnu inteligenciju za prediktivnu analizu prijetnji i optimizaciju IoT sustava (SEALSQ, 2024).
- **WISECoin:** platforma za tokenizaciju i autentifikaciju. WISECoin, je dio WISEKey ekosustava. Integrira AI, IoT i blockchain tehnologije. Ova platforma omogućuje sigurne digitalne interakcije između ljudi, uređaja i strojeva koristeći blockchain za autentifikaciju i umjetnu inteligenciju za analizu i validaciju identiteta (Wisekey, 2020).
- **SEALCOIN:** decentralizirana platforma koja objedinjuje IoT, blockchain i autonomne transakcije. AI se koristi za analizu podataka i optimizaciju transakcija između IoT uređaja, čime

se omogućuju autonomne i sigurnije interakcije (Sealcoin, 2024).

Sva ova inovativna rješenja doprinose području digitalne sigurnosti i učinkovitosti.

6. Zaključak

Integracija umjetne inteligencije (AI), interneta stvari (IoT) i blockchain tehnologije nudi značajna poboljšanja u digitalnoj sigurnosti financijskog sektora. AI omogućava analizu velikih količina podataka u stvarnom vremenu, proaktivno predviđanje prijetnji te brzu reakciju na sigurnosne incidente. IoT donosi podatke iz stvarnog svijeta u digitalne procese, omogućujući praćenje i zaštitu mrežnih aktivnosti u realnom vremenu. Blockchain pruža decentraliziranu, nepovredivu infrastrukturu koja osigurava transparentnost i sigurnost transakcija, dok pametni ugovori automatiziraju procese smanjujući rizik od ljudskih pogrešaka.

Kombiniranjem ovih tehnologija financijske institucije mogu stvoriti robustan sigurnosni okvir koji unaprjeđuje povjerenje korisnika i klijenata. Trenutno je objavljen relativno mali broj radova koji se bave ovom integracijom, ali se može očekivati povećano zanimanje i razvoj istraživanja u narednim godinama, kako ove tehnologije budu dobijale na značaju. Međutim, izazovi poput sigurnosnih ranjivosti, kompleksnosti implementacije i nedostatka stručnjaka zahtijevaju kontinuirana istraživanja i unaprjeđenja. Implementacija preporučenih mjera, uključujući enkripciju, autentifikaciju, redovito ažuriranje sustava i kriptografsku verifikaciju, može dodatno smanjiti rizike i osigurati stabilnije i sigurnije financijsko okruženje.

Rezultati istraživanja ukazuju na to da integracija umjetne inteligencije (AI), interneta stvari (IoT) i blockchain tehnologije donosi značajne koristi u unaprjeđenju digitalne sigurnosti financijskog sektora, čime se omogućuje odbacivanje nulte hipoteze i potvrđuje alternativna hipoteza.

Citirani izvori

- Alharbi, S., Attiah, A., & Alghazzawi, D. (2022). *Integrating Blockchain with Artificial Intelligence to Secure IoT Networks: Future Trends. Sustainability*, 14(23), 16002. doi:10.3390/su142316002
- Alloui, H., & Mourdi, Y. (2023). *Exploring the Full Potentials of IoT for Better Financial Growth and Stability: A Comprehensive Survey. Sensors*, 23(19), 8015. doi:10.3390/s23198015
- Alsirhani, A., Ezz, M., & Mostafa, A. M. (2022). *Advanced Authentication Mechanisms for Identity and Access Management in Cloud Computing. Computer Systems Science and Engineering*, 43(3), 967-984. doi:10.32604/csse.2022.024854
- Amazon. (2025, 04 04). AWS Cloud Services. Retrieved from AWS: <https://aws.amazon.com/products/>
- AWS. (2025, 04 03). AWS Lambda. Retrieved from Amazon: <https://aws.amazon.com/lambda/>
- Azure. (2025). *Find solutions for putting your ideas into action.* Retrieved from Microsoft: <https://azure.microsoft.com/en-us#solutions>
- Azure. (n.d.). *What is Azure.* Retrieved from Microsoft: <https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-azure/>
- Behm, S., Deetjen, U., Kaniyar, S., Methner, N., & Münstermann, B. (2019, 02 04). *Digital ecosystems for insurers: Opportunities through the Internet of Things.* Retrieved from McKinsey & Company: <https://www.mckinsey.com/industries/financial-services/our-insights/digital-ecosystems-for-insurers-opportunities-through-the-internet-of-things#/>
- Bogavac, M. (2019). *Research on the Influence of Digitalization on Small and Medium Enterprises.* Belgrade: ICIM+, Faculty of Business and Law, "Union - Nikola Tesla" University.
- Bwalya, K., & Paul, D. J. (2024, 10 02). *The Impact of Financial Technology on the Financial Services Industry: A Systematic Review. Heliyon - First Look*, 48.
- Cekerevac, Z., & Cekerevac, P. (2022, 07 15). *Blockchain and the application of blockchain technology.* (Z. Cekerevac, Ed.) *MEST Journal*, 10(2), 14-25. doi:10.12709/mest.10.10.02.02
- Cekerevac, Z., & Cekerevac, P. (2023, July 15). *Blockchain Technology and Application – SMEs Aspect.* (Z. Cekerevac, Ed.) *MEST Journal*, 11(2), 28-39. doi:10.12709/mest.11.11.02.04
- Cekerevac, Z., Dvorak, Z., Prigoda, L., & Cekerevac, P. (2017). *Internet of things and the Man-In-The-Middle attacks – Security and economic risks.* *MEST Journal*, 5(2), 15-25. doi:10.12709/mest.05.05.02.03

- Cekerevac, Z., Dvorak, Z., Prigoda, L., & Cekerevac, P. (2018). Hacking, protection and consequences of hacking. *Komunikacije Communications*, 20(2), 83-87.
- Cekerevac, Z., Prigoda, L., & Maletic, J. (2018, July 15). *Blockchain Technology and Industrial Internet of Things in the Supply Chains*. (Z. Cekerevac, Ed.) *MEST Journal*, 6(2), 39-47. doi:10.12709/mest.06.06.02.05
- Chilamkurti, N., Poongodi, T., & Balusamy, B. (Eds.). (2024). *Blockchain, Internet of Things, and Artificial Intelligence*. Chapman & Hall.
- Choucair, C. (2025, 02 18). WISEKey Unifies AI, Blockchain, and Quantum-Resistant Security to Strengthen Digital Trust. Retrieved from Quantum Computing Business: <https://thequantuminsider.com/2025/02/18/wisekey-unifies-ai-blockchain-and-quantum-resistant-security-to-strengthen-digital-trust/>
- Choucair, C. (2025, 02 18). WISEKey Unifies AI, Blockchain, and Quantum-Resistant Security to Strengthen Digital Trust. Retrieved from Quantum Insider: <https://thequantuminsider.com/2025/02/18/wisekey-unifies-ai-blockchain-and-quantum-resistant-security-to-strengthen-digital-trust/>
- Cisco. (2018, 12 17). *Blockchain by Cisco*. Retrieved from Cisco: <https://www.crowdfundinsider.com/wp-content/uploads/2019/03/Cisco-blockchain-whitepaper.pdf>
- Cisco. (2024, 12 16). What Is Secure Access Service Edge (SASE)? Preuzeto sa Cisco: <https://www.cisco.com/c/en/us/products/security/what-is-sase-secure-access-service-edge.html#~sase-overview>
- Coston, I., Plotnizky, E., & Nojournian, M. (2025). Comprehensive Study of IoT Vulnerabilities and Countermeasures. *Applied Sciences*, 15(6), 3036. doi:10.3390/app15063036
- Čekerevac, Z., & Bogavac, M. (2022). Impact of the pandemic on blockchain and the IoT application in supply chains from the SME aspect. *Mechanics Transport Communications*, 20(3/3), 11-17.
- Čekerevac, Z., Matić, S., Djurić, D., Čelebić, D. i Dvorak, Z. (2010). SDD ITG 'smart shelf' RFID rešenje za inventarisanje robe na udaljenim policama [Eng. SDD ITG smart shelf RFID solution for the stocktaking of goods on remote shelves]. *IMK-14 - Istraživanje i razvoj*, 47-52.
- Dallinger, L. (2024, 04 10). IoT in InsurTech: Revolution of the Insurance Industry. Retrieved from RTInsights: <https://www.rtinsights.com/iot-in-insurtech-revolution-of-the-insurance-industry/>
- Darktrace. (2021, 04 08). Preparing IT Professionals for AI Cyber Attacks. Retrieved from Darktrace: <https://www.darktrace.com/news/96-of-it-and-security-professionals-preparing-for-ai-powered-cyber-attacks-4>
- Devi, M., & Majumder, A. (2020). Side-Channel Attack in Internet of Things: A Survey. *Applications of Internet of Things* (pp. 213-222). Singapore: Springer. doi:10.1007/978-981-15-6198-6_20
- EclipseForensics. (2024, 12 18). The Significance of Cyber Deception Technologies in Detecting and Analyzing Cyber Threats. Preuzeto sa EclipseForensics: <https://eclipseforensics.com/the-significance-of-cyber-deception-technologies-in-detecting-and-analyzing-cyber-threats/?form=MG0AV3>
- Finnegan, O., White, J., Armstrong, B., E. L. Adams, S. B., Bastyr, M., Zhu, X., . . . Weaver, R. G. (2024). The utility of behavioral biometrics in user authentication and demographic characteristic detection: a scoping review. *Systematic Reviews*, 13, Article number 61. doi:10.1186/s13643-024-02451-1
- GDPR. (2024, 04 22). General Data Protection Regulation (GDPR). Retrieved 04 03, 2025, from <https://gdpr-info.eu/>
- Glöckler, J., Sedlmeir, J., Frank, M., & Fridgen, G. (2024). A Systematic Review of Identity and Access Management Requirements in Enterprises and Potential Contributions of Self-Sovereign Identity. *Business & Information Systems Engineering*, 421-440. doi:10.1007/s12599-023-00830-x
- Huawei. (2025). The Smart Future Is Here: Winning the Next Decade on HUAWEI CLOUD AI. Retrieved from Huawei Cloud: https://www.huaweicloud.com/intl/en-us/cloudplus/thirdphase/detail_05.html
- IBM. (2024, 05 16). IBM Support for Hyperledger Fabric. Retrieved from IBM: <https://www.ibm.com/products/blockchain-platform-hyperledger-fabric>
- IBM. (2024, 07 09). IBM Watson to watsonx - 70 years advancing AI. Retrieved from IBM: <https://www.ibm.com/watson>
- IBM. (2024, 12 27). What is homomorphic encryption? Preuzeto sa IBM: <https://www.ibm.com/think/topics/homomorphic-encryption>
- Intel. (2024, 02 26). Intel Announces New Edge Platform for Scaling AI Applications. Preuzeto sa intel: <https://www.intc.com/news-events/press-releases/detail/1679/intel-announces-new-edge-platform-for-scaling-ai>

- Intel Corporation. (2018, 11 26). *Blockchain Technology - Moving Beyond The Hype*. Retrieved from intel: <https://www.intel.com/content/dam/www/public/us/en/documents/brief/blockchain-business-brief.pdf>
- Intel Corporation. (2022, 12 14). *Accelerate Critical Edge Workloads with Built-in AI and Security Capabilities*. Retrieved from Intel: <https://www.intel.com/content/dam/www/central-libraries/us/en/documents/2022-12/iot-4th-gen-xeon-sp-product-brief.pdf>
- Jaćimovski, S., Šetrajčić, J., & Lamovec, J. (2019). O kvantnoj kriptografiji. *Žurnal za bezbjednost i kriminalistiku*, 1(1), 41-52.
- Jidong, D., & Yaqing, M. (2018, 02). *OceanConnect: Cloud IoT for the Future*. Retrieved from Huawei: <https://www.huawei.com/en/huaweitech/publication/84/ocean-connect-cloud-iot>
- Kataria, S. (2025, 03 06). *Secure and Transparent Cloud Solutions*. Retrieved from Services Quality Redefined: <https://www.qservicesit.com/azure-blockchain-powering-secure-and-transparent-cloud-solutions>
- Kumar, N., Joshi, S., & Alwan, A. S. (2023). *Impact of IoT on banking and financial services*. AIP Conference Proceedings. AIP Publishing. doi:10.1063/5.0170918
- Levin, B. (2024, 11 17). *What is Zero Trust Architecture (ZTA)?* Palo Alto. (N. Kumar, Interviewer) Retrieved from Paloalto: <https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture>
- Madiarbekova, A. (2025, 01 15). *Cybersecurity in IoT Devices: Vulnerabilities, Risks, and Mitigation Strategies*. KeAi - First Look, 13. doi:10.2139/ssrn.5075016
- Malatji, M., & Tolah, A. (2024, 02 15). *Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI*. *AI Ethics*. doi:10.1007/s43681-024-00427-4
- Mohamed, N. (2023, 10 25). *Current trends in AI and ML for cybersecurity: A state-of-the-art survey*. *Cogent Engineering*. doi:10.1080/23311916.2023.2272358
- Nilay, D. (2024, 10 28). *How IoT Transforms Finance: Applications & Benefits [2024]*. Retrieved from intuz: <https://www.intuz.com/blog/iot-impact-financial-services-industry>
- Nofel, M., Marzouk, M., Elbardan, H., Saleh, R., & Mogahed, A. (2024). *Integrating Blockchain, IoT, and XBRL in Accounting Information Systems: A Systematic Literature Review*. *Journal of Risk and Financial Management*, 17(8), 372. doi:10.3390/jrfm17080372
- Puah, R. (2022, 07 08). *The World of Interoperability — Cosmos vs Polkadot*. Preuzeto sa Switcheo: <https://blog.switcheo.com/the-world-of-interoperability-cosmos-vs-polkadot/>
- Rane, N., Choudhary, S., & Rane, J. (2023, 12 01). *Blockchain and Artificial Intelligence (AI) Integration for Revolutionizing Security and Transparency in Finance*. doi:10.2139/ssrn.4644253
- Sajid, H. (2024, 05 03). *Prijetnja ofenzivne umjetne inteligencije i kako se od nje zaštititi*. Retrieved from Unite.ai: <https://unite.ai/hr/prijetnja-ofenzivnog-AI-ja-i-kako-se-od-njega-za%C5%A1tititi/>
- Sealcoin. (2024). *Empowering IoT with Secure, Decentralized Transactions*. Retrieved from Sealcoin: <https://sealcoin.ai/>
- SEALSQ. (2024, 12 02). *SEALSQ and Parent Company WISEKey Advance AI Integration*. Retrieved from SEALSQ: <https://www.sealsq.com/investors/news-releases/sealsq-and-parent-company-wisekey-advance-ai-integration>
- Sharma, S., Selvi, G. P., Shailaja, M. L., Mehta, A., Srivastva, A., & Gupta, A. (2024). *Smart Contracts and Blockchain: Integrating AI and IoT for Transparent Banking Transactions*. *Journal of Informatics Education and Research*, 4(3), 2152.
- Siddhartha, V., Gaba, G. S., & Kansal, L. (2020). *A Lightweight Authentication Protocol using Implicit Certificates for Securing IoT Systems*. *Procedia Computer Science*, 85-96. doi:10.1016/j.procs.2020.03.185
- Skoromets, S. (2024, 04 24). *Fraud Detection Using AI in Banking: AI Model Explained*. Retrieved from Eliftech: <https://www.eliftech.com/insights/fraud-detection-using-ai-in-banking/>
- Som, A., & Kayal, P. (2022). *AI, Blockchain, and IOT. In Digitalization and the Future of Financial Services, Innovation and Impact of Digital Finance (pp. 141-161)*. doi:10.1007/978-3-031-11545-5_8
- Soundenkar, S., Bhosale, K., Jakhete, M. D., Kadam, K., Chowdary, V. G., & Durga, K. (2024). *AI Powered Risk Management: Addressing Cybersecurity Threats in Financial Systems*. *Library Progress International*, 44(3). doi:10.48165/bapas.2024.44.2.1
- Suresh, R., & Manoj, K. (2024). *Fintech: Revolutionizing financial service through digital platforms*. *International Journal of Research in Financial Management*, 562-566. doi:10.33545/26175754.2024.v7.i2f.410

- techblog. (2022, 11 10). Vodič za IoT u bankarstvu i Fintech-u. Retrieved from TechBlog.co.rs: <https://techblog.co.rs/vodic-za-iot-u-bankarstvu-i-fintech-u/>
- Tubin, G. (2024, 11 20). Security Automation: Tools, Process and Best Practices. Preuzeto sa Cynet: <https://www.cynet.com/incident-response/security-automation-tools-process-and-best-practices/>
- Vaideswaran, N. (2025, 03 12). A Comprehensive Survey on Data Loss Prevention (DLP). Preuzeto sa CrowdStrike: <https://www.crowdstrike.com/en-us/cybersecurity-101/data-protection/data-loss-prevention-dlp/>
- Venkatachalam, S., & Siraj, A. (2019, 04 16). Unlock the Value of Data with Cisco Kinetic (IoT). Retrieved from Cisco: https://www.cisco.com/c/dam/m/en_sg/events/connect-2019/pdfs/unlock-the-value-of-data.pdf
- Vignette, V. (2019, 10 24). Cisco Blockchain. Retrieved from Deep Analysis: <https://www.deep-analysis.net/wp-content/uploads/2019/11/DA-V-1910-Cisco-blockchain-no-distribution.pdf>
- Wisekey. (2020, 12 21). WISECoin, the Innovative Tokenized Service of WISEKey, Authenticates People, Products and Machines Using Blockchain and AI. Retrieved from Wisekey: <https://www.wisekey.com/press/wisecoin-the-innovative-tokenized-service-of-wisekey-authenticates-people-products-and-machines-using-blockchain-and-ai/>
- XiaoJun, Z. (2025). HUAWEI CLOUD Blockchain Technology – Building Trust in Industry Applications. Retrieved from Huawei Cloud Computing Technologies Co.: https://www.huaweicloud.com/intl/en-us/cloudplus/secondphase/detail_15.html
- Yarter, M., Uehara, G., & Spanias, A. (2022). Implementation and Analysis of Quantum Homomorphic Encryption. 2022 13th International Conference on Information, Intelligence, Systems & Applications (IISA) (str. 1-5). IEEE Xplore. doi:10.1109/IISA56318.2022.9904399
- Yilmaz, N. K., & Hazar, H. B. (2019). THE RISE OF INTERNET OF THINGS (IoT) AND ITS APPLICATIONS IN FINANCE AND ACCOUNTING. PressAcademia Procedia, 10(1), 32-35.
- Zhao, W., Alwidian, S., & Mahmoud, Q. H. (2022). Adversarial Training Methods for Deep Learning: A Systematic Review. Algorithms, 15(8), 283.
- Zulhusni, M. (2024, 12 23). How blockchain, IoT, and AI are shaping the future of digital transformation. Retrieved from AINews: <https://www.artificialintelligence-news.com/news/how-blockchain-iot-and-ai-are-shaping-the-future-of-digital-transformation/>

Safer Finances: How AI, IoT, and Blockchain Revolutionize Digital Security

Summary

The integration of artificial intelligence (AI), the Internet of Things (IoT), and blockchain technology represents a significant step forward in enhancing digital security within the financial sector. AI enables real-time analysis of large datasets, threat detection, automated security responses, and risk prediction based on historical data, thereby advancing proactive security measures. IoT brings real-world data into digital processes, allowing for monitoring of network activities, swift responses to anomalies, and personalized services through smart devices. Blockchain ensures data immutability via decentralized ledgers, providing transparency, transaction security, and resilience against cyber-attacks. Smart contracts further automate processes, reducing the risk of fraud and human error. Despite current challenges, such as security vulnerabilities, implementation complexities, and the relatively limited number of published studies on this integration, the combination of these technologies holds the potential to create advanced security systems. This combination not only strengthens resilience against threats but also enhances user and client trust. This paper serves as a valuable starting point for future research to further illuminate the possibilities and challenges of integrating AI, IoT, and blockchain in the financial sector. Interest in this topic is expected to grow in the coming years as these technologies evolve and see broader global application.

Keywords: Artificial Intelligence (AI), Internet of Things (IoT), Blockchain, Digital Security, Financial Sector