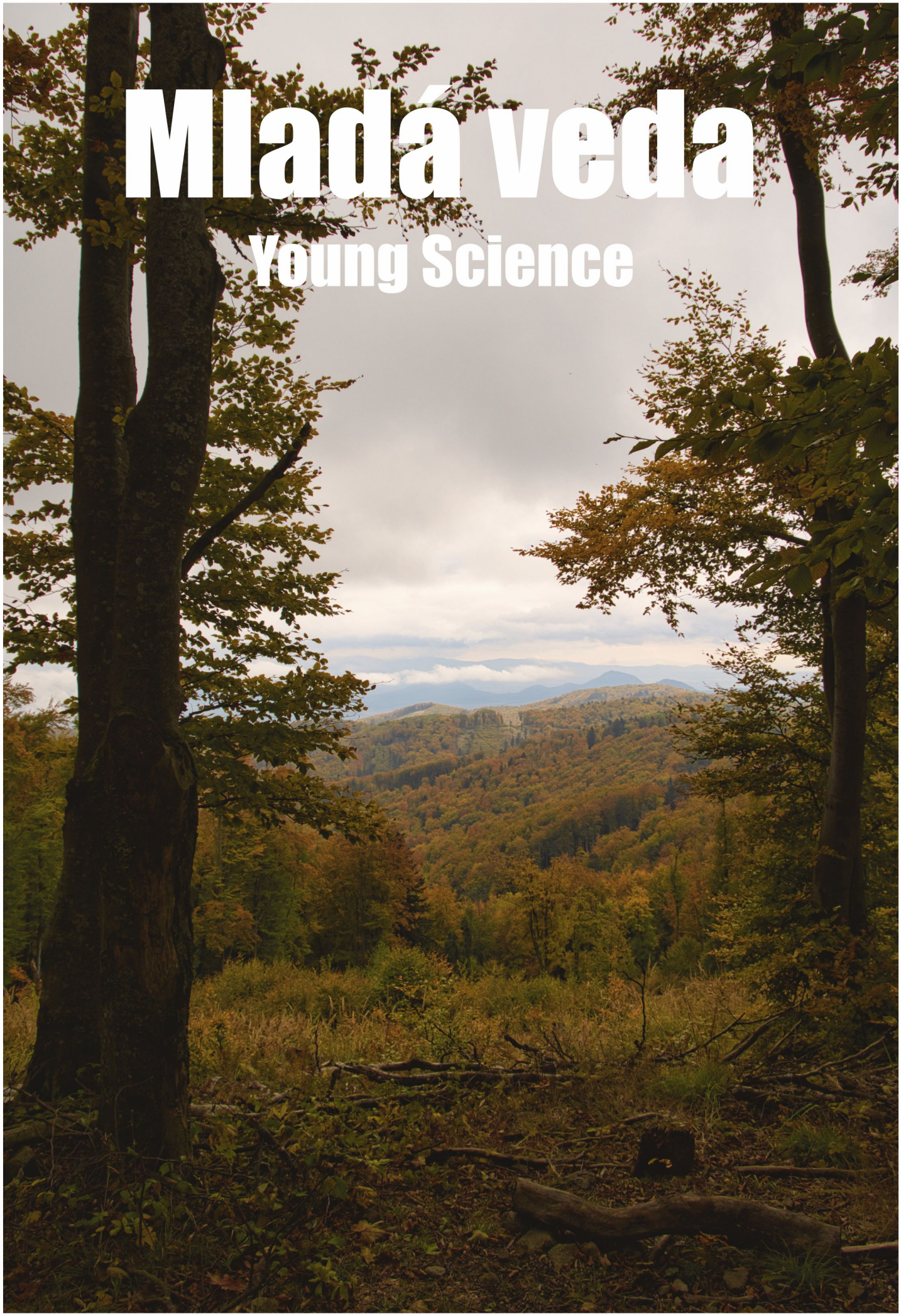
ISSN 1339-3189 5/2026

Mladá veda

Young Science



www.mladaveda.sk

Mladá veda
Young Science

MEDZINÁRODNÝ VEDECKÝ ČASOPIS MLADÁ VEDA / YOUNG SCIENCE
Číslo 5, ročník 14., vydané v septembri 2026
ISSN 1339-3189, EV 167/23/EPP
Kontakt: info@mladaveda.sk, tel.: +421 908 546 716, www.mladaveda.sk
Fotografia na obálke: Pohorie Čergov. © Branislav A. Švorc, foto.branisko.at

VYDAVATEĽ
Inštitút pre vedu, kultúru a spoločenský rozvoj
IČO: 57728038, Bajkalská 12B, 080 01 Prešov, Slovensko
v spolupráci s vydavateľstvom UNIVERSUM-EU, spol. s r. o.

Mladá veda
Young Science
ISSN 1339-3189

Vol. 14 (5), pp. 67-73

BEZPEČNOSTNÉ RIZIKÁ DECENTRALIZOVANÝCH APLIKÁCIÍ (DAPPS) Z POHĽADU POUŽÍVATEĽA

SECURITY RISKS OF DECENTRALIZED APPLICATIONS (DAPPS) FROM THE USER PERSPECTIVE

Libor Jakubec[1]

Autor pôsobí ako doktorand na Vysokej škole bezpečnostného manažérstva v Košiciach. Vo svojej dizertačnej práci sa venuje bezpečnému používaniu kryptomien v bežnom živote.

The author is a doctoral candidate at the University of Security Management in Košice. In his dissertation, he focuses on the secure use of cryptocurrencies in everyday life.

Abstract
The article examines the security risks of decentralized applications (dApps) from the perspective of a regular user. While the transition from centralized services provides greater control over digital assets, it also places full responsibility for key management and account protection on the user. Today's most significant threats do not arise from technical vulnerabilities in smart contracts, but from manipulation, social engineering, and careless transaction confirmation. The text outlines a multi-layered protection approach involving rigorous URL verification, limiting token approvals, utilizing pre-signature transaction analysis tools, and distributing assets across different types of wallets. The conclusion emphasizes that in the trustless Web3 environment, high digital literacy, constant vigilance, and disciplined behavior are essential to preventing irreversible losses.
Key words: decentralized applications, dApps, Web3, cybersecurity, smart contracts

Abstrakt
Článok sa venuje bezpečnostným rizikám decentralizovaných aplikácií (dApps) z pohľadu bežného používateľa. Prechod od centralizovaných služieb síce prináša väčšiu kontrolu nad digitálnymi aktívami, no zároveň kladie na používateľa plnú zodpovednosť za správu kľúčov a ochranu účtov. Najvýraznejšie hrozby dnes nevznikajú z technických chýb smart kontraktov, ale z manipulácie, sociálneho inžinierstva a nepozorného potvrdzovania transakcií. Text uvádza postup založený na viacvrstvovej ochrane, v podobe dôsledného overovania webových adries, obmedzovania tokenových oprávnení, využívania nástrojov na analýzu transakcií pred podpisom a rozdelenia aktív medzi rôzne typy peňaženiek. Záver zdôrazňuje, že v

[1] Adresa pracoviska: Ing. Libor Jakubec, Ústav humanitných a technologických vied, Vysoká škola bezpečnostného manažérstva v Košiciach, Košťova 1, 040 01 Košice
E-mail: jakubec@itznalec.sk

bezdôverovom prostredí Web3 je kľúčová vysoká digitálna gramotnosť, neustála ostražitosť a disciplinované správanie, aby sa predišlo nenahraditeľným stratám.
Kľúčové slová: decentralizované aplikácie, dApps, Web3, kybernetická bezpečnosť, smart kontrakty

Úvod

Decentralizované aplikácie (dApps) sa stali jedným z kľúčových prvkov rozvíjajúceho sa ekosystému Web3. Na rozdiel od tradičných webových služieb nefungujú na centrálnych serveroch, ale na distribuovaných blockchainových sieťach, kde logické operácie a pravidlá interakcie zabezpečujú smart kontrakty. Tento model odstraňuje potrebu sprostredkovateľov a používateľom poskytuje väčšiu kontrolu nad ich digitálnymi aktívami aj nad samotnými transakciami. S touto technologickou zmenou však prichádza aj zásadná zmena v oblasti bezpečnosti a zodpovednosti. Kým v centralizovaných systémoch je bezpečnosť a správa prostriedkov v rukách jednotlivých inštitúcií, vo svete Web3 preberá túto úlohu samotný používateľ. Model vlastnej správy aktív znamená, že každý jednotlivec je plne zodpovedný za svoje kľúče, transakcie a rozhodnutia. Keďže operácie na blockchaine sú nezvratné, aj malé pochybenie môže viesť k trvalej strate prostriedkov. V posledných rokoch sa ukazuje, že najväčšie riziká už nevyplývajú z technických chýb v samotných smart kontraktoch, ale z nedostatočnej informovanosti používateľov, prípadne zo zneužitia ich dôvery. Phishing, manipulácia používateľského rozhrania či nepozorné schvaľovanie transakcií sa stali dominantnými aspektami útokov. Tento trend predstavuje významnú prekážku pre širšie využitie decentralizovaných technológií, pretože bezpečnosť ekosystému je dnes do veľkej miery závislá od správania a digitálnej gramotnosti koncových používateľov.

Jadro

Blockchain predstavuje distribuovanú databázovú architektúru, ktorá zabezpečuje nemenné a transparentné ukladanie údajov. Decentralizované aplikácie (dApps) na tejto infraštruktúre stavajú a využívajú smart kontrakty na automatizované vykonávanie procesov bez centrálneho riadenia. Rozvoj programovateľných blockchainov, umožnil vznik komplexných aplikácií fungujúcich v decentralizovanom výpočtovom prostredí. Smart kontrakty sú programy uložené priamo v blockchaine, ktoré sa vykonávajú automaticky podľa vopred definovaných pravidiel. Ich základnými vlastnosťami sú nemennosť, transparentnosť a autonómnosť. Hoci tieto charakteristiky zvyšujú dôveryhodnosť systému, zároveň vytvárajú riziko, pretože chyby v kóde nie je možné po nasadení jednoducho opraviť. Bezpečnosť smart kontraktov sa tak stáva kľúčovým faktorom pri návrhu a prevádzke dApps, keďže ich zraniteľnosti môžu mať priamy dopad na integritu digitálnych aktív používateľov (Szabo, 1997).

Transformácia od centralizovaných systémov Web2 k „trustless“ architektúram Web3 zásadne mení spôsob, akým sa pristupuje k bezpečnosti. Kým v tradičnom modeli zodpovedá za ochranu dát a prostriedkov poskytovateľ služby, decentralizované aplikácie fungujú bez centrálnej autority a odstraňujú sprostredkovateľov. Tento posun zavádza model vlastnej správy, v ktorom používateľ kontroluje svoje privátne kľúče, podpisuje transakcie a sám rozhoduje o interakciách so smart kontraktmi. Zodpovednosť za bezpečnosť tak prechádza výhradne na jednotlivca, ktorý je vystavený rizikám, aké predtým riešili špecializované

bezpečnostné tímy. Web3 preto vyžaduje výrazne vyššiu úroveň digitálnej gramotnosti, keďže používateľ v praxi preberá úlohu vlastnej banky aj vlastného bezpečnostného oddelenia (Sun et al., 2026).

Rýchly rast dApps v posledných rokoch priniesol výrazné inovácie v oblastiach ako DeFi či DAO, no zároveň aj citeľný nárast kybernetických útokov. Počet incidentov v blockchainovom prostredí sa medziročne zvyšuje o stovky percent a celkové straty sa už pohybujú v miliardách dolárov, čo jasne ukazuje, že bezpečnosť z pohľadu používateľa je kritickou témou (tabuľka 1). Interakcia s dApp totiž nie je obyčajné používanie softvéru, ale séria kryptografických autorizácií, ktoré priamo ovplyvňujú vlastníctvo digitálnych aktív. Celý proces prebieha medzi frontendom aplikácie, používateľskou peňaženkou a smart kontraktmi na blockchaine. Práve v tomto reťazci vznikajú slabé miesta, ktoré sa snažia útočníci zneužiť (Binance, 2024).

Popis	Hodnota	Trend (oproti roku 2019)
Celkový počet incidentov v roku 2020	555	nárast o 240 %
Ekonomické vyčíslenie podvodov	7,8 miliardy USD	nárast o 82 %
Straty z uskutočnených hackerských útokov	3,2 miliardy USD	nárast o 516 %
Ukradnuté prostriedky z protokolov	viac ako 3 miliardy USD	pretrvávajúca zraniteľnosť infraštruktúry

Tabuľka 1 - Bezpečnostné incidenty
Zdroj: Nominis, 2026; Anand, 2026

Podstata dApp spočíva v prepojení nemenných smart kontraktov s bežným webovým rozhraním, pričom blockchain slúži ako dôveryhodný záznam. Štruktúra zahŕňa dve vrstvy interakcie. Po prvé je to interakcia používateľ vs. frontend a po druhé interakcia smart kontrakt vs. sieť. Otvorený kód zvyšuje transparentnosť, ale zároveň uľahčuje útočníkom analýzu jednotlivých slabín. Používateľ sa pripája peňaženkou namiesto hesla, čo eliminuje riziká únikov prihlasovacích údajov, no prináša výzvy v správe kľúčov a autorizácii transakcií. V prípade ak užívateľ celkom nerozumie významu a podstate pojmov ako gas, slippage alebo allowance môže to viesť k vážnym chybám. Vzhľadom na nemennosť kontraktov majú možnosti zraniteľnosti (reentrancy, overflow, chyby prístupovej logiky) často nezvratné následky, a to aj napriek auditom a bug bounty programom (Sun et al., 2026; Sonule, 2025).

Bezpečnosť v decentralizovanom svete nie je jednorazový cieľový stav, ale je to nepretržitý proces ostražitosti a správneho používania digitálnych aktív. Na základe analýzy súčasných hrozieb je nevyhnutné, aby používatelia dApps prijali komplexnú a hlavne viacvrstvovú bezpečnostnú stratégiu.

Bezpečná interakcia so smart kontraktmi si vyžaduje dôsledný technický postup a systematické overovanie všetkých krokov pred podpisom transakcie. Kľúčovým prvkom je preverovanie zdrojov, z ktorých používateľ získava informácie, pričom odkazy by mali pochádzať výhradne z oficiálnych komunikačných kanálov projektu. Súčasťou tohto procesu

je aj kontrola URL adries, keďže rôzne formy typosquattingu patria medzi najčastejšie phishingové techniky. Riziko je možné výrazne znížiť používaním uložených záložiek namiesto manuálneho zadávania adries. Pri prvom kontakte s novou decentralizovanou aplikáciou je vhodné realizovať testovaciu transakciu s nízkou hodnotou a pri udeľovaní povolení pracovať len s presne definovanými sumami tokenov. Schvaľovanie neobmedzených oprávnení predstavuje významné riziko, pretože v prípade kompromitácie môže útočník získať plný prístup k aktívam používateľa. Rovnako dôležitá je následná správa týchto oprávnení. Po ukončení interakcie, najmä s menej etablovanými protokolmi, by mali byť udelené povolenia bezodkladne zrušené. Pravidelná kontrola, ideálne v určitých denných intervaloch, výrazne obmedzuje priestor na zneužitie. Na tento účel možno využiť špecializované nástroje, ktoré poskytujú prehľad o všetkých aktívnych oprávneniach a umožňujú ich jednoduché odvolanie (Si, J. J. et al., 2024).

V oblasti ochrany používateľov pred pokročilými formami phishingu zohrávajú dôležitú úlohu analytické a simulačné nástroje, ktoré pôsobia ako sprostredkujúca vrstva medzi decentralizovanou aplikáciou a peňaženkou. Ich úlohou je rozložiť pripravovanú transakciu na zrozumiteľné prvky a ešte pred podpisom odhadnúť jej výsledok, čím dokážu včas upozorniť na podozrivé alebo neštandardné operácie. Medzi najpoužívanejšie riešenia patria bezpečnostné rozšírenia, ako napríklad Pocket Universe, Blockaid či Scam Sniffer, ktoré identifikujú rizikové podpisy vrátane pokročilých schém typu Permit2 alebo rôznych off-chain autorizácií. Tieto nástroje zároveň dokážu interpretovať aj zložitejšie interakcie, napríklad operácie so stakovanými aktívami. Významnú úlohu zohrávajú aj peňaženky s integrovanou simuláciou transakcií, ako je Rabby Wallet. Tá poskytuje používateľovi jasnú predikciu výsledku operácie v čitateľnej podobe a upozorňuje na interakcie s neznámymi či rizikovými kontraktmi. Za základné pravidlo sa považuje, že ak peňaženka alebo simulačný nástroj nedokáže transakciu analyzovať a predpovedať jej dôsledky, mala by byť považovaná za vysoko rizikovú a používateľ by mal od jej podpisu upustiť (Svein, 2024).

Základným odporúčaním pre každého používateľa dApps a jedným z najúčinnejších prístupov k ochrane digitálnych aktív je ich dôsledné rozdelenie podľa účelu a úrovne rizika, ktorému sú vystavené. Tento model pracuje s viacerými typmi peňaženiek, pričom každá z nich plní odlišnú funkciu. Peňaženka určená na každodenné používanie, často označovaná ako „horúca“ alebo „interakčná“ a slúži na bežné transakcie, prípadne na testovanie nových dApps. Mala by obsahovať len nevyhnutné množstvo prostriedkov a jednotlivé oprávnenia je potrebné pravidelne kontrolovať. Na dlhodobé a bezpečné uchovávanie aktív sa využívajú hardvérové peňaženky, ktoré fungujú v režime offline. Tieto zariadenia by sa nemali pripájať k decentralizovaným aplikáciám ani používať na podpisovanie bežných operácií. Ak je potrebné presunúť prostriedky, odporúča sa smerovať ich výhradne na vlastnú, overenú interakčnú peňaženku. Pri správe väčších objemov aktív, ako sú napríklad prostriedky organizácií alebo dlhodobé úspory, sa za najbezpečnejšie riešenie považujú multisig peňaženky. Každá transakcia v tomto modeli vyžaduje schválenie viacerými nezávislými kľúčmi, čo výrazne znižuje riziko straty majetku v prípade kompromitácie jedného zariadenia alebo účtu. Takto nastavená segregácia aktív predstavuje robustný základ pre bezpečné fungovanie vo Web3 prostredí (Binance, 2024).

Pred každým podpisom transakcie alebo správy je potrebné dodržať niekoľko kontrolných krokov, ktoré výrazne znižujú riziko neoprávnených operácií. Prvým z nich je dôkladná kontrola webovej adresy, najmä s ohľadom na možné preklepy či imitácie legitímnych domén, a overenie bezpečnostných certifikátov. Ideálne je pracovať s vopred uloženými odkazmi, aby sa minimalizovala možnosť presmerovania na falošné stránky. Rovnako dôležité je vyhodnotenie simulačného náhľadu transakcie. Ak peňaženka alebo bezpečnostné rozšírenie nedokáže predpovedať výsledok operácie, je potrebné považovať takúto transakciu za mimoriadne rizikovú. Pri udeľovaní povolení by mal používateľ vždy nastaviť presný limit tokenov potrebných na konkrétnu operáciu, namiesto akceptovania predvoleného neobmedzeného prístupu, ktorý predstavuje výrazné bezpečnostné riziko. Po ukončení interakcie s menej známymi alebo novými protokolmi je vhodné udelené oprávnenia okamžite zrušiť. Tým sa eliminuje možnosť ich neskoršieho zneužitia a uzatvára sa potenciálny priestor pre neoprávnené manipulácie s aktívami používateľa. Tento postup predstavuje základný rámec bezpečného správania pri práci s decentralizovanými aplikáciami (Sun et al., 2026; Binance, 2024).

Do budúcnosti sa očakáva, že bezpečnostné mechanizmy v oblasti decentralizovaných aplikácií sa budú posúvať od reaktívnych opatrení k proaktívnym stratégiám. Jedným z hlavných smerov je integrácia umelej inteligencie, ktorá umožňuje priebežné monitorovanie on-chain správania a identifikáciu anomálií naznačujúcich potenciálne útoky či podvodné mechanizmy typu „rug pull“. Moderné modely dokážu analyzovať veľké objemy transakcií v reálnom čase a odhaliť neštandardné vzorce, ktoré by ľudský audítor zachytil len s výrazným oneskorením. Súčasne sa rozvíjajú modulárne blockchainové architektúry, ktoré oddeľujú výpočtovú vrstvu od vrstvy konsenzu a dátovej dostupnosti. Tento prístup umožňuje prispôsobiť úroveň bezpečnosti konkrétnemu typu aplikácie. Finančné protokoly môžu využívať robustnú ochranu hlavnej siete, zatiaľ čo aplikácie orientované na rýchlosť môžu fungovať na špecializovaných rollupoch. Avšak takáto flexibilita však zároveň zvyšuje zložitosť komunikácie medzi reťazcami, čo otvára nové možnosti pre útoky na mosty a cross-chain infraštruktúru. Významný posun sa očakáva aj v oblasti správy digitálnych identít. Princípy Zero Trust a decentralizované identifikátory umožnia používateľom preukazovať určité vlastnosti či oprávnenia bez toho, aby museli odhaľovať svoje osobné údaje. Overiteľné kredenciály a dôkazy s nulovým zverejnením informácií (ZKP) tak môžu poskytnúť vyššiu úroveň súkromia a zároveň splniť požiadavky regulačných rámcov. Tento trend smeruje k modelu, v ktorom kontrola nad identitou a dátami prechádza z platforiem späť na používateľov, čo je jedným zo základných princípov Web3, no zároveň si vyžaduje nové štandardy ochrany súkromia a vzájomnú kompatibilitu blockchainov (Stohniev, 2026; Welch, 2026).

Záver

Bezpečnosť decentralizovaných aplikácií možno v stručnosti charakterizovať ako určité napätie medzi bezprecedentnou mierou slobody a rovnako bezprecedentnou mierou zodpovednosti. Decentralizované aplikácie dApps prinášajú do digitálneho prostredia nové formy finančnej suverenity, transparentnosti a prístupu k inovatívnym službám, zároveň však zásadne menia charakter kybernetických hrozieb. Trend vývoja útokov v posledných rokoch naznačuje, že pozornosť útočníkov sa postupne presúva od hľadania komplexných zraniteľností v kóde smart

kontraktov k zneužívaniu autorizačných mechanizmov, používateľského rozhrania a sofistikovaným formám phishingu. Prevažná časť finančných strát tak už nevzniká v dôsledku technického zlyhania infraštruktúry, ale najmä v dôsledku ľudskej chyby, nepozornosti a nesprávnych návykov pri práci s peňaženkou a dApps. Je preto potrebné si jasne uvedomiť, že blockchain neposkytuje záruku bezpečnosti v zmysle ochrany pred chybnými rozhodnutiami používateľa. Garantuje len presné a nezvratné vykonanie inštrukcií zapísaných v kóde a ak používateľ neuvážene podpíše škodlivú transakciu alebo udelí neobmedzené oprávnenie k svojim aktívam, sieť túto operáciu vykoná korektne, no jej dôsledky sú často nenapraviteľné. V tomto zmysle sa koncový používateľ stáva najslabším, ale zároveň rozhodujúcim článkom celého bezpečnostného reťazca. Web3 stavia na paradigme, podľa ktorej je jednotlivec zároveň vlastnou bankou aj vlastným bezpečnostným oddelením, čo si vyžaduje mieru zodpovednosti porovnateľnú so správou fyzického trezoru. Bezpečné a dlhodobo udržateľné používanie decentralizovaných aplikácií preto nemožno vnímať ako otázku náhody, ale ako výsledok disciplinovaného prístupu, systematickej ostražitosti a priebežného vzdelávania. Kľúčovú úlohu zohráva obmedzovanie udelených oprávnení, dôsledné overovanie zdrojov a opatrnosť pri každej jednej interakcii. V prostredí bez centrálnej autority, ktorá by dokázala vrátiť odcudzené prostriedky, sa stáva základným pravidlom zásada, že všetko je potrebné si dvakrát overiť a podpísať až vtedy, keď presne užívateľ rozumie dôsledkom svojej akcie.

Tento článok odporúčal na publikovanie vo vedeckom časopise Mladá veda:
Dr.h.c. prof. Ing. Josef Reitšpís, CSc., DBA, MSc.

Použitá literatúra

1. ANAND, 2026. *Understanding dApp Security Risks and the Best Prevention Strategies.* [online]. [cit. 2026-02-19]. Dostupné z: https://www.nadcab.com/blog/dapp-security-risks-prevention-strategies
2. BINANCE, 2024. *Web3 Security: The Danger of Unlimited Approvals on Ethereum Virtual Machine Chains.* [online]. [cit. 2026-02-14]. Dostupné z: https://www.binance.com/en/blog/security/6629495486558213511
3. NOMINIS, 2026. *NOMINIS Monthly Report: Crypto Hacks and Attacks in January 2026.* [online]. [cit. 2026-02-19]. Dostupné z: https://www.nominis.io/insights/nominis-monthly-report-crypto-hacks-and-attacks-in-january-2026
4. SI, J. J. et al., 2024. *Understanding User-Perceived Security Risks and Mitigation Strategies in the Web3 Ecosystem.* [online]. [cit. 2026-02-21]. Dostupné z: https://dl.acm.org/doi/fullHtml/10.1145/3613904.3642291
5. SONULE, N., 2025. User Experience (UX) in Web3 and DApps: Challenges and Opportunities. In: *International Journal of Scientific Harmonization of Digital Horizons.* [online]. Roč. 2025, č. 1, s. 1-3 [cit. 2026-02-10]. ISSN 3108-1495 Dostupné z: https://stwilfredscollege.co.in/uploads/4_ij_shodh_journal_24_july_2025.docx_Niraj_Sonule.pdf
6. STOHNIEV, H., 2026. *The Industrialization of Decentralized Logic: Comprehensive Real-World Use Cases for Smart Contracts and dApps in 2026.* [online]. [cit. 2026-03-14]. Dostupné z: https://ideasoft.io/blog/real-world-use-cases-for-smart-contracts-and-dapps/
7. SUN, H. et al., 2026. *From Data Behavior to Code Analysis: A Multimodal Study on Security and Privacy Challenges in Blockchain-Based DApp.* [online]. [cit. 2026-02-16]. Dostupné z: https://arxiv.org/html/2504.11860v2
8. SVEIN, 2024. *The Best Web3 Wallet Comparison: Find the Perfect Wallet for You.* [online]. [cit. 2026-02-25]. Dostupné z: https://blog.kryll.io/best-web3-wallet-comparison-which-is-best/

9. SZABO, N., 1997. Formalizing and Securing Relationships on Public Networks. In: *First Monday*. Roč. 2, č. 9, s. 1-35. ISSN 1396-0466
10. WELCH, P. M., 2026. *Data Protection Strategies for 2026.* [online]. [cit. 2026-03-12]. Dostupné z: https://hyperproof.io/resource/data-protection-strategies-for-2026/

Mladá veda

Young Science

ISSN 1339-3189