Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 4.9
DOI: https://doi.org/10.24867/34BE04Gligorov

ARHITEKTURA BEZBEDNOG DIGITALNOG NOVČANIKA SA VIŠESTRUKIM POTPISIMA

ARCHITECTURE OF A SECURE MULTI-SIGNATURE WALLET

Nevena Gligorov, *Fakultet tehničkih nauka, Novi Sad*

Oblast – ELEKTROTEHNIKA I RAČUNARSTVO

Kratak sadržaj – *U ovom radu će biti analizirana arhitektura bezbednih digitalnih novčanika, sa glavnim naglaskom na novčanike sa višestrukim potpisima. Rad uključuje i predlog arhitekture digitalnog novčanika sa višestrukim potpisima u sistemima elektronskog plaćanja.*

Ključne reči: *digitalni novčanik, e-novčanik, digitalni novčanik sa višestrukim potpisom, arhitektura, bezbednost*

Abstract – *This paper will present an analysis of the architecture of secure digital wallets, with the main focus on multisignature digital wallets. The paper also includes a proposal for an architecture of a secure multisignature digital wallet that could be used in electornic payment systems.*

Keywords: *digital wallet, e-wallet, multi-signature digital wallet, architecture, security*

1. UVOD

Trgovina je evoluirala od razmene materijalnih dobara i zlatnika do savremenih digitalnih sistema plaćanja. *Fintech* revolucija sa sobom je donela mobilno bankarstvo koje omogućava brz i jednostavan uvid u stanje računa i izvršavanje transakcija putem mobilnog telefona. Uz to, sve veću popularnost počeli su da dobijaju sistemi elektronskog plaćanja i korišćenje kriptovaluta. Glavni zahtev ovih sistema jeste očuvanje bezbednosti visokog nivoa. U te svrhe, nastali su digitalni novčanici sa višestrukim potpisima, čija bezbednost se temelji na korišćenju podeljene odgovornosti nad sredstvima. Tehnologija se kontinuirano razvija, a sa njom i sistemi plaćanja koji zajedno sa digitalnim novčanicima tek treba da dostignu svoj vrhunac upotrebe [1, 2].

2. TEORIJSKE OSNOVE I KORIŠĆENE TEHNOLOGIJE

2.1. Platni instrument

Platni instrument predstavlja skup informacija koje opisuju neku ekonomsku vrednost, a koji je potreban odgovarajućem protokolu radi izvršavanja transakcije elektornskog plaćanja.

2.2. Elektronski novac

Elektronski novac je novac koji može (npr. evro), ali i ne mora (npr. kriptovalute) imati svoju fizičku reprezentaciju, a čija je osnovna namena korišćenje u sistemima elektronskog plaćanja, u okviru kog i omogućava sam proces plaćanja.

Kirptovaluta je ime dato sistemu koji koristi kriptografiju kako bi se proces slanja podataka izvršio na siguran način. Pored toga, sistem takođe koristi kriptografiju radi distribucije digitalnih tokena u raštrkanom maniru [3].

Kako bi mogao da se koristi u sistemima elektronskog plaćanja, elektronski novac mora biti: univerzalno prihvaćen, transferabilan, deljiv, takav da ga je nemoguće falsifikovati ili ukloniti bez odgovarajuće autorizacije, privatan (niko sem korisnika koji učestvuje u transakciji nema uvid u njenu vrednost), anoniman (korisnik koji vrši plaćanje se ne može identifikovati) i takav da se valuta može koristiti i kada sistem nema pristup *Internet* mreži, odnosno, da ne zahteva *online* verifikaciju [4].

2.3. *Blokčejn*

Blokčejn predstavlja javni zapisnik (engl. *public ledger*) svih izvršenih transakcija. Sastoji se iz blokova, gde svaki blok iz mreže referencira na heš vrednost svog bloka prethodnika (roditeljskog bloka). Blok se sastoji od tela, u okviru kojeg se nalaze transakcije i njihov brojač, ali i zaglavlja koje sadrži: verziju bloka, heš vrednost roditeljskog bloka, heš vrednost korena Merkleovog stabla, vreme, *nBits* i *Nonce*.

Osnovna karakteristika *Blokčejn* mreže jeste da je ona decentralizovana, perzistentna, anonimna i da ima mogućnost revizije. Razlog zbog kojeg se mreža pokazala dobro u okviru decentralizovanih sistema je zato što koristi heš funkciju za enkriptovanje, digitalni potpis zasnovan na asimetričnoj kriptografiji, kojim se vrši potvrda identiteta i konzenus protokol.

Blokčejn mreže omogućavaju realizaciju elektronskog plaćanja bez potrebe za postojanjem posrednika, poput banaka kod kartičnog plaćanja, čime se povećava efikasnost i smanjuje cena izvršavanja čitavog procesa plaćanja [5].

2.4. Sistemi elektronskog plaćanja

Sistem elektronskog plaćanja obuhvata sve transakcije, odnosno, plaćanja izvršena elektronskim putem. Danas, jedan od veoma popularnih načina kupovine jeste *online*

NAPOMENA:
Ovaj rad proistekao je iz master rada čiji mentor je bio dr Dušan Gajić, vanr. prof.

kupovina, koja je realizovana upravo upotrebom ovog sistema, a uz pomoć koje krajnji korisnik uživa u pogodnostima kupovine iz svog doma.

Svaki sistem elektornskog plaćanja koji nudi različite opcije za izvršavanje procesa kupovine, mora ispunjavati stroge kriterijume upotrebljivostio, prihvaljivosti, skalabilnosti, interoperabilnosti, dostupnosti i bezbednosti.

Kao jedno od večito aktuelnih tema, pitanju bezbednosti se i kod tradicionalnih i kod elektronskih sistema plaćanja mora pristupiti veoma ozbiljno. Bezbednost se može posmatrati kao niz zahteva koje je potrebno ispuniti, poput: prevencije od prevare, poverljivosti i otpornosti na greške. Krajnji korisnik, odnosno, njegove lične informacije i sredstva u novčaniku u svakom momentu moraju biti zaštićeni, tako da ne postoji nijedan način kojim bi se napadači mogli koristiti da se tih istih sredstava, odnosno, informacija dokopaju. Takođe, ukoliko dođe do iznenadnog pada sistema, to ni na koji način ne sme uticati na korisnika. Kako su sve transakcije koje se izvršavaju atomične, u ovom slučaju bi to značilo prosto poništavanje svi do tada izvršenih koraka, čime se rezervisani deo korisnikovih sredstava ne gubi [6].

Postoji jako puno različitih tehnologija i načina koji se mogu koristiti za implementaciju jednog digitalnog novčanika. U ovom radu, iako je glavni fokus na digitalnim novčanicima sa višestrukim potpisima, ukratko će biti i opisana ideja integracije standardnog digitalnog novčanika u okviru mobilnog telefona, čiji rad se zasniva na upotrebi *NFC* i *NDEF* tehnologija u okviru *Android* operativnog sistema, kao što je opisano u radu [4]. S druge strane, moguće je kreirati interoperabilni digitalni novčanik opisan u [7] koji se zasniva na korišćenju *IFPS*, *SHA256* i *blokčejn* tehnologija.

Poput *Electrum* digitalnog novčanika [8] moguće je koristiti *Python*, P*yQt6*, *Kivy*, *libsecp256k1* i *QML* kako bi se realizovao novčanik koji podržava i jednostruke i višestruke potpise. Pored njega, sličnu podršku daju i *Sparrow Wallet* [9], koji za svoju implementaciju koristi *PSBT, Java (JDK 17+), JavaFX, HWI*, *Drongo, OpenPNP, Hummingbird, Lark, DuckDB secp256k1* i *ZBar*, i *Safe Smart Account* [10] koji se bazira na korišćenju *TypeScript*, *Solidity*, *Python* i pametnih ugovora.

U [11] se predlaže implementacija digitalnog novčanika sa višestrukim potpisima kojim se upotrebom *Bloom* filtera, *T-ECDSA* algoritma i *Multi-praty ECDSA* postiže viši nivo bezbednost, uz očuvanje performansi standardnih digitalnih novčanika.

3. ANALIZA BEZBEDNOG DIGITALNOG NOVČANIKA SA VIŠESTRUKIM POTPISIMA

Digitalni novčanik predstavlja servis namenjen elektronskom plaćanju koji izdaje izdavalac (engl. *issuer*) koji je nezavisan od bilo koje transakcije. Sadrži podatke o platnom instrumentu, kao i sva sredstva neophodna za izvršavanje online transakcija. Bez obzira da li je reč o digitalnim novčanicima sa jednim ili više potpisa, kako bi se ostvarila brza i efikasna transakciona komunikacija, novčanik mora biti: proširiv, simetričan, ne čisto *web* namenjen, klijentski orijentisan i pre svega, bezbedan. Arhitektura većine gotovih rešenja koja se danas koriste ne podržava svaku od prethodno navedenih stavki, jer bi takva implementacija bila veoma zahteva, zbog čega se često pravi kompromis u implementiranim i neimplementiranim delovima [3].

3.1. Digitalni novčanik sa jednim potpisom

Digitalni novčanik sa jednim potpisom je najčešće korišćeni tip digitalnih novčanika. Kontrola nad sredstvima u celosti zavisi samo od jednog korisnika, zbog čega je omogućena direktna i jednostavna kontrola nad digitalnom imovinom.

3.1.1. Digitalni novčanik integrisan u mobilni telefon

[4] predlaže kreiranje mobilne aplikacije koja bi predstavlja sistem elektrosnkog plaćanja u kom bi digitalni novčanik bio njegov sastavni deo. Korišćenjem *NFC* tehnologije moguće je izvršiti transfer novca iz jednog u drugi novčanik. Komunikacija, koja se još i naziva procesom zračenja, vrši se razmenom poruka uz pomoć *NDEF* tehnologije. Svaka poruka se sastoji od: količine novca koji se šalje, sertifikata valute (koristi se kao mehanizam bezbednosti uz pomoć kog se proverava validnost novca koji se transferuje, a u okviru ovog pristupa se smatra da svaka valuta ima svoj digitalni sertifikat), korisnika koji transferuje sredstva, korisnika koji prima sredstva i datum izvršavanja plaćanja.

Prednosti ovog pristupa su što, ukoliko primenjeno na veliki broj korisnika, ne postoji potreba za nošenjem fizičkog novčanika uz mobilni telefon, jer će se u okviru prenosnog uređaja nalaziti sve što je jednom korisniku potrebno. S druge strane, to je i jedna od glavnih mana, jer u slučaju gubitka mobilnog telefona, to efektivno znači i gubitak svih sredstava digitalnog novčanika.

3.1.2. Digitalni novčanik zasnovan na blokčejn tehnologiji

Moguće je kreirati standardni digitalni novčanik koji se zasniva na korišćenju *blokčejn* tehnologije, kao što je opisano u [7]. Arhitektura ovog pristupa se zasniva na korišćenju *miner* komponenti za svaku od banaka sistema, prilikom čega one predstavljaju računarski server vrhunskih performansi. Ideja je da svaka banka svojim klijentima izda digitalni novčanik, poput kartica koje se danas koriste, prilikom čega bi taj novčanik sadržao adrese svih *miner* komponenti sistema, ali i svoj privatni i javni ključ koji su mu potrebni za potpisivanje, odnosno, validaciju digitalnih potpisa. Banke sistema veruju jedna drugoj i koriste *POS* konsenzus protokol radi dogovaranja oko jedne verzije istine.

Prilikom plaćanja, kreira se transakcija koja sadrži količinu sredstava potrebnu za plaćanje, kao i digitalni potpis korisnika koji izvršava datu akciju, a koji je kreiran njegovim privatnim ključem. *Miner* komponente prihvataju tu transakciju, beleže je i nakon toga prebacuju novac iz bankovnog računa korisnika u njegov digitalni novčanik, prilikom čega se vrši provera da li korisnik uopšte ima dovoljno sredstava za izvršavanje transakcije. Ukoliko ima, *miner* komponente kreiraju još jednu transakciju koja simbolizuje prebacivanje sredstava, a koju sve ostale *miner* komponente beleže. Vrši se transfer sredstava iz jednog u drugi novčanik, gde je poslednji korak prebacivanje tih sredstava iz novčanika na račun primaoca.

Osnovna mana ovih novčanika jeste što imaju jednu glavnu kritičnu tačku, a to je korišćenje jednog privatnog ključa. U slučaju njegovog gubitka ili krađe od strane hakera, sva sredstva koja se nalaze u digitalnom novčaniku se nepovratno gube.

3.2. Digitalni novčanik sa višestrukim potpisima

Digitalni novčanici sa višestrukim potpisima nude rešenje problema bezbednosti, u okviru kog se realizuje deljena odgovornost nad sredstvima novčanika, odnosno, vrši se generisanje više različitih parova privatni/javni ključ koji se dodeljuju svakom od korisnika koji su vlasnici novčanika. Ovim putem se rešava slabost jedne kritične tačke standardnih digitalnih novčanika. Veoma je teško doći do jednog privatnog ključa, što postaje eksponencijalno teže sa porastom njihovog broja. Međutim, najveća mana ovog pristupa je što većina postojećih rešenja zahteva izmene u protokolima koji se koriste, ili čak i upotrebu pametnih ugovora, što utiče na performanse čitavog sistema [11].

3.3. Postojeća rešenja

3.3.1. *Electrum*

Electrum je manje zahtevna (engl. *lightweight*) verzija *Bitcoin* digitalnog novčanika, koju je 2011. godine kreirala i objavila kompanija *Electrum Technologies GmbH* [12]. Podržava kreiranje i korišćenje standardnih digitalnih novčanika, ali i novčanika sa višestrukim potpisima.

Kreira i održava desetak konekcija ka serverima, od kojih se samo jedan koristi kao glavni, dok ostali služe za dobijanje informacija vezanih za transakcione naknade. Glavni server se koristi za praćenje aktivnosti vezanih za deljene novčanike, kao i uvrštavanje transakcije u *blokčejn* mrežu.

Svaki od korisnika dobija svoj par privatnog i javnog ključa, prilikom čega se privatni ključ generiše na osnovu slučajno generisane fraze. Da bi transakcija bila odobreno, prilikom kreiranja novčanika definiše se *n* korisnika koji će deliti sredstva, od kojih je samo *m* potrebno da digitalno potpiše transakciju kako bi se ona smatra odobrenom [8].

Arhitekturu ovog novčanika je moguće ugrubo podeliti na pet modula: prezentacioni, aplikacioni, biznis logiku, mrežni i *Bitcoin* mrežni modul. Prezentacioni modul sadrži sva podešavanja neophodna za korišćenje desktop aplikacije kojom se novčanik reprezentuje, dok se u aplikacionom modulu nalazi glavna logika. Mrežni modul je namenjen održavanju konekcije sa *Electrum* serverima, dok se *Bitcoin* mrežni modul koristi za komunikaciju *Electrum* novčanika sa *bitcoin* mrežom [13].

3.3.2. *Sparrow wallet*

Sparrow wallet je desktop aplikacija koja predstavlja *Bitcoin* novčanik koji je podržan na većini hardverskih novčanika. Bazira se na korišćenju popularnih standarda poput *PBST*, pri čemu je akcenat stavljen na transparentnosti i upotrebljivosti novčanika [14].

Podržava dva režima rada: sa i bez pristupa mreži, kao i konekciju na tri različita tipa servera: javni server, *Bitcoin Core* čvor i privatni *Electrum* server. Ovi server nude različite nivoe bezbednosti i kompleksnosti, pa su iz tog razloga i namenjeni različitim tipovima korisnika.

Podržava kreiranje digitalnih novčanika sa višestrukim potpisima, prilikom čega se svakom od *n* korisnika kreira novčanik sa privatnim i javnim ključem, a za odobravanje transakcije potrebno i dovoljno je usaglašavanje samo *m* korisnika [9].

Na osnovu otvorenog koda ovog digitalnog novčanika [14] moguće je definisati njegovu arhitekturu, koja se sastoji iz: prezentacionog i aplikacionog sloja, sloja *Drongo* biblioteke, skladišta, mrežnog sloja, hardverskog sloja i niza eksternih zavisnosti, potrebnih za funkcioniasnje čitavog sistema.

Upravljanje novčanicima, transakcijama i svim događajima vrši aplikacioni sloj, a za potrebe enkapsulacije logike *Bitcoin* protokola se koristi *Drongo* biblioteka [15].

3.3.3. Digitalni novčanik sa višestrukim potpisima i *Bloom* filterom

Potrebno je dizajnirati digitalni novčanik sa višestrukim potpisima koji unapređuje aspekt bezbednosti standardnih digitalnih novčanika, ali ne na račun performansi, kao što to obično biva kog novčanika sa višestrukim potpisima. U te svrhe, predložen je novčanik [11] koji vrši rekonstrukciju višestrukih potpisa, tako da se od njih kreira jedan digitalni potpis koji *blokčejn* mreža može brzo proveriti. Na ovakav način se višestrukim digitalnim potpisima postiže očuvanje povećane bezbednosti koju imaju digitalni novčanici višestrukih potpisa, ali se njihovom rekonstrukcijom obezbeđuje očuvanje performansi sistema.

Rekonstrukcija digitalnih potpisa se postiže korišćenjem algoritma digitalnih potpisa zasnovanim na korišćenju praga eliptične krive *T-ECDSA*. Provera validnosti dobijenog potpisa omogućena je upotrebom *Bloom* filtera koji se šalje u okviru transakcije umesto svih javnih ključeva korisnika. Osim što zauzima manje prostora nego javni ključevi, ovaj filter eliminiše nepotrebno slanje personalnih informacija putem javnog ključa. Uz pomoć *Bloom* filtera moguće je i dobiti uvid u učesnike prilikom potpisivanje transakcije.

Arhitektura ovog sistema se može podeliti na klijentsku i serversku stranu, kod koje je serverska zadužena za razmenu javnih i enkriptovanih ključeva. U okviru njega vrši se pomenuta rekonstrukcija potpisa, kao i njegova validacija. S druge strane, klijentska strana sadrži različite module za enkripciju i dekripciju, generisanje ključeva i transakcija, kao i potpisivanje, komunikaciju i validaciju.

3.3.4. *Safe Smart Account*

Safe Smart Account je digitalni račun sa integrisanim funkcionalnostima digitalnih novčanika sa višestrukim potpisima, zbog čega se često i nazivaju digitalnim novčanicima. Predstavlja jedan od vodećih primera digitalnih novčanika *Ethereum* mreže.

Na osnovu otvorenog koda [10] izvodi se zaključak da se glavna logika u radu ovog tipa novčanika zasniva na korišćenju pametnih ugovora. Arhitekturu *Safe* novčanika moguće je podeliti u nekoliko slojeva. Klijentski sloj omogućava različite načine upravljanja digitalnim računima. Glavni sloj (engl. *Core layer*) predstavlja srž arhitekture. Dizajniran je prema *proxy pattern* principu,

čija je osnovna ideja odvajanja stanja novčanika od njegove logike. Integracioni sloj omogućava proširenja funkcionalnosti sistema dodavanjem novih, ali tako da one nikako ne utiču na osnovna ponašanja čitavog sistema. Dizajniran je po principu odvojenih odgovornosti (engl. *separation of concerns*), tako da je svaka komponenta nezavisna od ostalih i od osnovnog sistema.

Poslednji sloj je *Blokčejn* sloj koji predstavlja infrastrukturu sa kojom *Safe Smart Account* komunicira, odnosno, u okviru koje vrši emitovanje i izvršavanje transakcija i ugovora sistema.

3.4. Integracija u sistem elektronskog plaćanja

U sistem elektronskog plaćanja koji korisnicima omogućava plaćanje putem kartice banke ili *QR* koda, upotrebom *PayPal* servisa ili *Ethereum* kriptovalute, moguće je integrisati digitalni novčanik sa višesturkim potpisima uz pomoć kog bi se povećala bezbednost celokupnog sistema, ali ne na račun njegovih performansi. Uz pomoć ovog novčanika bi se izbacila potreba za postojanjem dodatnih učesnika u komunikaciji, kao što to obično biva kod kartičnog plaćanja. Po uzoru na opisane novčanike, moguće je kreirati arhitekturu digitalnog novčanika sa višestrukim potpisima koji bi se bazirao na kreiranju odvojenih računa za svaki način plaćanja, a koji bi jedan modul u kome se nalazi celokupna logika. Rekonstrukcijom višestrukih potpisa, moguće je kreirati jedan potpis, za koji je potrebno odrediti odgovarajući mehanizam validacije. Time bi se omogućila bezbednost visokog nivoa, uz izbacivanje redudantne implementacije sličnih procesa obrađivanja transakcija.

4. ZAKLJUČAK

Digitalni novčanici sa višestrukim potpisima predstavljaju rešenje koje adresira probleme bezbednosti sistema elektronskih plaćanja. Oni eliminišu slabosti standardnih rešenja i omogućavaju transparentan način upravljanja sredstvima u okviru timova i organizacija.

Trenutno opisani sistem predstavlja idejno rešenje čija je dalja razrada potrebna. Nakon definisanja tehnološkog steka i implementacije svih funkcionalnosti, potrebno je izvršiti obimno testiranje i tek nakon optimizacionih korigovanja, moguće je razmatranje implementacije digitalnog novčanika u realni sistem elektronskog plaćanja.

LITERATURA

[1] M. A. Hassan and Z. Shukur, “Review of Digital Wallet Requirements,” in *2019 International Conference on Cybersecurity (ICoCSec)*, Sept. 2019, pp. 43–48. doi: 10.1109/ICoCSec47621.2019.8970996.

[2] S. Sukaris, W. Renedi, M. A. Rizqi, and B. Pristyadi, “Usage Behavior on Digital Wallet: Perspective of the Theory of Unification of Acceptance and Use of Technology Models,” *J. Phys. Conf. Ser.*, vol. 1764, no. 1, p. 012071, Feb. 2021, doi: 10.1088/1742-6596/1764/1/012071.

[3] T. Handayani and A. Novitasari, “Digital Wallet as a Transaction Media in The Community,” *IOP Conf. Ser. Mater. Sci. Engl.*, vol. 879, no. 1, p. 012001, July 2020, doi: 10.1088/1757-899X/879/1/012001.

[4] O. Dospinescu, “E-Wallet. A New Technical Approach,” *Acta Univ. Danub. Œcon.*, vol. 8, no. 5, pp. 84–94, 2012.

[5] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, “Blockchain challenges and opportunities: a survey,” *Int. J. Web Grid Serv.*, Oct. 2018, doi: 10.1504/IJWGS.2018.095647.

[6] A.-R. Sadeghi and M. Schneider, “Electronic Payment Systems,” in *Digital Rights Management: Technological, Economic, Legal and Political Aspects*, E. Becker, W. Buhse, D. Günnewig, and N. Rump, Eds., Berlin, Heidelberg: Springer, 2003, pp. 113–137. doi: 10.1007/10941270_9.

[7] K. Singh, N. Singh, and D. Singh Kushwaha, “An Interoperable and Secure E-Wallet Architecture based on Digital Ledger Technology using Blockchain,” in *2018 International Conference on Computing, Power and Communication Technologies (GUCON)*, Sept. 2018, pp. 165–169. doi: 10.1109/GUCON.2018.8674919.

[8] “Welcome to the Electrum Documentation! — Electrum 4 documentation.” Accessed: Oct. 09, 2025. [Online]. Available: https://electrum.readthedocs.io/en/latest/

[9] “Documentation,” Sparrow Wallet. Accessed: Oct. 12, 2025. [Online]. Available: https://sparrowwallet.com/docs/

[10] “safe-global/safe-smart-account at release/v1.5.0,” GitHub. Accessed: Oct. 13, 2025. [Online]. Available: https://github.com/safe-global/safe-smart-account

[11] J. Han, M. Song, H. Eom, and Y. Son, “An efficient multi-signature wallet in blockchain using bloom filter,” in *Proceedings of the 36th Annual ACM Symposium on Applied Computing*, in SAC ’21. New York, NY, USA: Association for Computing Machinery, Apr. 2021, pp. 273–281. doi: 10.1145/3412841.3441910.

[12] “Electrum (software),” *Wikipedia*. Aug. 25, 2025. Accessed: Oct. 09, 2025. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Electrum_(software)&oldid=1307780521

[13] *spesmilo/electrum*. (Oct. 11, 2025). Python. spesmilo. Accessed: Oct. 11, 2025. [Online]. Available: https://github.com/spesmilo/electrum

[14] *sparrowwallet/sparrow*. (Oct. 11, 2025). Java. Sparrow Wallet. Accessed: Oct. 11, 2025. [Online]. Available: https://github.com/sparrowwallet/sparrow

[15] *sparrowwallet/drongo*. (Oct. 10, 2025). Java. Sparrow Wallet. Accessed: Oct. 13, 2025. [Online]. Available: https://github.com/sparrowwallet/drongo

Kratka biografija:

Nevena Gligorov rođena je u Kraljevu 2001. god. Diplomski rad na Fakultetu tehničkih nauka u Novom Sadu iz oblasti Elektrotehnike i računarstva – Računarstvo i automatika odbranila je 2024. god. kontakt: gligorov.nevena@gmail.com