Vlastimir Vuković

# Otkrivanje anonimnosti u modernim plaćanjima

CBM *Research*, Paper 7, mart 2023

*/S a ž e t a k/*

Anonimnost plaćanja i privatnost transaktora nije se spominjala pre kraja 20. veka, niti je anonimnost isticana kao karakteristika novca. Preokret počinje 1990-ih sa pojavom elektronskog novca, zatim Bitcoina 2008. i brojnih kriptovaluta 2010-ih. U današnje vreme monetarne analize anonimnost stavljaju u najvažnije karakteristike novca, kao najvažniji uslov privatnosti plaćanja. Međutim, istraživanje anonimnosti plaćanja u istorijskoj perspektivi pokazuje da je većina transakcija, gotovinskih ili bezgotovinskih, bila dokumentovana, odnosno neanonimna. Zato se današnji moderni elektronski sistemi plaćanja u svetu još uvijek oslanjaju na Hamurabijev princip dokumentovanog novca, a ne na Nakamotovu ideju o kriptografskom dokazu.

Postavlja se pitanje kako su svi naučni autoriteti tokom vekova prevideli tako važnu karakteristiku novca i plaćanja kao što je anonimnost? Kako se čuvala privatnost transaktora uprkos dominaciji neanonimnih dokumentovanih plaćanja? Zašto se anonimnost uvek potcenjivala i povezivala samo sa svakodnevnim maloprodajnim plaćanjima male vrednosti? Generalni odgovor je da anonimnost plaćanja nije bitna jer se privatnost transaktora podrazumevala sve do 1940-ih godina. To je ujedno i odgovor na prvo pitanje. Treba li verovati Smitu, Torntonu, Dževonsu, Mengeru, Vikselu, Fridmanu i ostalim istraživačima novca ili anonimnom Satošiju Nakamotu i promoterima deljenja podataka i otvorenog bankarstva?

*Anonimnost plaćanja*

Reči anonimnost i privatnost teško se mogu pronaći od Hamurabija do 1990-ih. Zaokret je započeo uvođenjem elektronskog novca za širu javnost i potiskivanjem gotovine iz maloprodajnih transakcija. Međutim, potpuni preokret pokrenut je 2008. godine kada je anonimni autor (ili autori) Satoši Nakamoto obnarodovao Bitcoin kao *decentralizovani protokol plaćanja zasnovan na kriptografskom dokazu*. Ubrzo zatim lansiran je čitav niz drugih tzv. kriptovaluta, čiji broj i danas raste. Na taj je način javnosti nasilno nametnuta tema anonimnosti novca i privatnosti plaćanja.

Emitenti kriptovaluta iz *fintech* sektora od početka su isticali anonimnost kao ključni dokaz nadmoći kripto novca u odnosu na novac banaka. Komercijalne banke bile su pasivni posmatrači, jer se ubrzo pokazalo da su kriptovalute špekulativna imovina sa izrazito nestabilnom tržišnom vrednošću, koje se najmanje korišćene za plaćanja.

Novi talas inovacija započeli su *stablecoin* projekti, čiji su glavni pokretači bile vodeće *bigtech* platforme, sa milijardama članova, svakodnevnih korisnika njihovih usluga. To je prisililo tehnološki inertne centralne banke da počnu razmišljati o sopstvenoj digitalnoj valuti – digitalnoj

[*] Ovaj rad je kraća verzija diskusionog papira ***Hamurabi protiv kriptovaluta: anonimnost plaćanja*** , DP br. 3, *Istraživanje novca centralne banke* , novembar 2022.

valuti centralne banke (CBDC). Erupcija CBDC projekata započela je u junu 2019. kada je *Facebook* otkrio svoju nameru da emituje sopstveni globalni *stablecoin*. U početnoj fazi sve centralne banke naglašavale su anonimnost kao ključnu odliku budućih CBDC-ova za maloprodajna plaćanja manje vrednosti, najavljujući tako svoj odgovor na pretnje *bigtech* platformi. Na taj je način anonimnost postala središte trougla kriptovalute-stablecoin-CBDC i krunski argument u konkurentskoj trci tri sektora - *fintech*, *bigtech* i bankarstva.

Danas većina monetarnih analiza svrstava anonimnost u jednu od najvažnijih odlika novca, koja presudno utiče na privatnost plaćanja. Da li je reč o izvanrednoj monetarnoj inovaciji ili o kriptografijom maskiranom pokušaju emitenata kriptovaluta da preuzmu bar deo senjoraže i veći deo plaćanja od povlašćenog bankarskog sektora? Činjenica da svi postojeći elektronski sistemi plaćanja u svetu, maloprodajni i veleprodajni, još uvijek počivaju na Hammurabijevom principu dokumentovanog *novca* nedvosmisleno negira svaki poseban značaj anonimnosti za novčane transakcije.

Anonimnost je uvek bila povezana s gotovinom u maloprodajnim plaćanjima male vrednosti. Zato je ovo kriptografsko glorifikovanje anonimnosti od 2008. izgledala anahrono. Međutim, kolosalna medijska promocija kriptovaluta postavila je anonimnost na pijedestal na kome nikada nije bila. Tome je posebno doprinelo neosnovano izjednačavanje (pseudo)anonimnosti plaćanja i privatnosti transaktora. Neanonimnost plaćanja nije pretnja privatnosti, već *mobilnost podataka* koji skriva otvoren *pristup* i anarhično *deljenje podataka* .

Važnost anonimnosti koju ističu *fintech* i *bigtech* entiteti očito je hipertrofirana kako bi služila u marketinške svrhe. Slično naglašavanje anonimnosti u radovima brojnih istraživača digitalnog novca nema uporište u monetarnoj istoriji i modernim sistemima plaćanja. Konačno, ne postoji identičnost između anonimnosti plaćanja i privatnosti.

*Anonimnost plaćanja u istorijskoj perspektivi*

Postojanje *dokumentovanog novca* može se videti već u 18. veku stare ere u Vavilonskom Carstvu. Njegovo značenje, metod i obuhvat u drevnom trgovanju objašnjava *Hamurabijev zakonik*. Ovaj najstariji pravni kodeks na svetu obvezuje agente i trgovce da izdaju i prime *potvrdu za novac* (§104 i §105). Anonimnost novčanih transakcija u Hamurabijevom Vavilonu očigledno je bila potcenjena.

Od otkrića kovanog novca, anonimnost plaćanja bila je uglavnom odlika bronzanih kovanica. "Bronza nije predstavljala problem jer je bila rezervisana za *male apoene za lokalnu upotrebu*" (Finley, str. 167). Zbog neznatne intrinzičke vrednosti nije bilo potrebe da menjači ispituju njihovu težinu i čistoću, kao u slučaju kovanica od plemenitih metala. Korišćenje zlatnih i srebrnih kovanica tokom antike, uključujući poklone i nasledstva, bilo je uglavnom dokumentovano, tj. neanonimno.

Pojava depozitara – *trapezita* u Atini u drugoj polovini petog veka i *argentarija* u Rimu krajem četvrtog veka stare ere (Andreau, str. 30), svedoči o ranim slučajevima dokumentovanih bankarskih transakcija u antici. Suvišno je dokazivati da tadašnje bankarstvo i današnje transakcije novčanim depozitima nisu mogle biti anonimne, iako su se u to vreme obavljale deponovanjem

gotovine u obliku zlatnika i srebrnjaka. Transakcije su bile dokumentovane u *bankarskom registru računa* (ibid, str. 46).

"Bilo je beskrajnog pozajmljivanja novca među Grcima i Rimljanima" (Finley, str. 141, 198). Jasno je, kao i u slučaju depozita, da su ove *beskrajne* kreditne transakcije morale biti evidentirane u gore spomenutom *bankarskom registru računa* (Andreau, str. 39-40, 44). Takva praksa je bila u skladu sa rimskim pravnim sistemom koji nije poznavao anonimne depozite i kredite.

Većina drugih plaćanja većih vrednosti – plaćanja imanja, za aukcijske prodaje, za porez, transport, osiguranje, proizvodnju, veleprodaju, stanovanje i slično, takođe nije bila anonimna, jer je trebalo imati dokaz o *uplati*. Očekivano, dokumentovana su i sva plaćanja javnih vlasti za vojsku, javne priredbe i javne zgrade.

Najveći porast anonimnosti plaćanja počinje nakon pada Rima, krajem petog veka i traje sve do desetog veka. Bio je to rani srednji vek ili mračni vek, obeležen dramatičnim padom svih ekonomskih aktivnosti, posebno trgovine i kovanja novca. Teška nestašica novca pogodila je sve delove bivšeg Zapadnog Rimskog Carstva. Vizantija je nastavila koristiti kovanice u svakodnevnim transakcijama i slediti rimsku tradiciju dokaza *plaćanja* za veće iznose. Kina takođe nije prekidala svakodnevnu upotrebu kovanica svih vrsta, metalnih i nemetalnih, niti praksu dokumentovanog novca u trgovačkim transakcijama.

Porast kovanica u opticaju "kada je poplava novog srebra postala dostupna u kasnom dvanaestom veku u Evropi" (Spufford, str. 243) nije mogao olakšati velike transakcije, koje su se obavljale u papiru i izmirivale u polugama srebra (ibid, str. 235). Bio je to početak jedinstvene *komercijalne revolucije*, temeljene na metodama kliringa i poravnanja u dokumentovanim transakcijama plaćanjima. Ovi neanonimni načini plaćanja promovisani su i razvijani na poznatim srednjovjekovnim sajmovima.

Glavni oslonac ove komercijalne revolucije bili su menjači novca koji su počeli primati depozite u kovanicama i polugama i dokumentovati ih u svojim knjigama na računima deponenata. To im je omogućilo transfer sredstava sa jednog računa na drugi prema nalozima svojih klijenata (Đenova, Venecija).

Osnivanjem triju javnih banaka u Evropi krajem 16. i početkom 17. veka – venecijanske Banco di Rialto (1587.), Bank of Amsterdam (1609.) i Bank of Hamburg (1610.) – započela je prava platna revolucija. Monetarni haos u cijeloj Evropi tako je obuzdan, obračunske jedinice stabilizovane, dok je depozitni novac ili *novac banaka* (depoziti u javnim bankama) učinio velika plaćanja jednostavnijim i sigurnijim. Plaćanja preko javnih banaka, kao pouzdanih posrednika, bila su po svojoj prirodi neanonimna.

Krajem 17. i tokom 18. veka Britanija je preuzela primat u inovacijama plaćanja. "Rastuća upotreba čekova upečatljiva je odlika londonskog privatnog bankarstva u drugoj polovini osamnaestog veka" (Richards, str. 192). Evolucija međubankarskih plaćanja izrodila je Bankarsku klirinšku kuću u Londonu 1770-ih, što je omogućilo privatnim bankarima da dovrše kliring i

poravnanje između deponenata odgovarajućim međusobnim transakcijama. Naravno, sve te transakcije bile su višestruko dokumentovane.

Tendencija pada udela kovanica i novčanica, kao sredstava za anonimna plaćanja u maloprodaji, bila je vidljiva u celom svetu sve do kraja 20. veka. Pojava elektronskog/digitalnog novca u svetu umreženom internetom uzrokovala je gubitak svake preostale anonimnosti plaćanja i otkrivanjem privatnosti pojedinaca.

*Uzdizanje anonimnosti*

Anonimnost kao najvažniju odliku novca i plaćanja otkrili su emitenti kriptovaluta. Preostale odlike bile su manje važne za podršku marketinškoj promociji njihovog kripto-novca. To je razlog zašto je nisu nazvali npr. investiciona valuta (što bi bilo najbliže istini) ili decentralizovana valuta (što bi takođe bilo bliže istini). Jednostavno, ništa ne može biti efektivnije od prefiksa kripto i obećanja anonimnih plaćanja.

Ekspanzija kriptovaluta od pojave Bitcoina do danas zasniva se na agresivnom isticanju anonimnosti. Teško je zamisliti da bi se cela ova industrija pojavila i opstala bez atributa anonimnosti.

Tržišni prodor novih emitenata nije ometala ni činjenica da je početna Nakamotova ideja u procesu realizacije iz osnova promenjena. Treća strana nije eliminisana (*rudari*), anonimnost je svedena na *pseudo anonimnost*, Bitcoin nije postao sredstvo plaćanja, već izrazito *špekulativno ulaganje*, dok kriptografski dokaz nije zamenio poverenje izvan kriptomreža. Uprkos svemu, ti nezavisni emitenti uživali su punu slobodu izdavanja "svojih" valuta s nekim nepoznatim pokrićem. Izuzete su iz propisa o inovacijama s nejasnim ishodom u neobuzdanoj hajekovskoj valutnoj konkurenciji.

*Anonimnost ili privatnost: da li je anonimnost neophodna?*

Osnovno pitanje je da li je moguća privatnost transaktora bez anonimnosti plaćanja? Istorija novca i plaćanja daje nepobitan odgovor: DA!

Konfuzija je nedvosmisleno prva reč u razmatranjima anonimnosti i privatnosti, kao i njihove međuzavisnosti. Da li je anonimnost plaćanja uslov privatnosti, kako tvrde emitenti kriptovaluta ili je obrnuto, kako tvrde neki istraživači? Da li je privatnost potpuna anonimnost? Problem je dodatno komplikovan istovremenim korišćenjem uslova anonimnosti i privatnosti za transakcije i transaktore. U teoriji, anonimnost je *odlika* transakcija, a privatnost je *pravo* transaktora. U praksi je obrnuto – anonimnost transaktora i privatnost transakcija.

Rašireno je mišljenje da se privatnost može osigurati anonimnošću transakcija za sve osobe i subjekte, uključujući drugog učesnika u transakciji i provajdera plaćanja! (Kahn, str. 338-9). *Uspostavljanje anonimnosti* u svakoj dokumentovanoj/zabeleženoj transakciji bilo bi teško izvodljivo čak i uz neku sveobuhvatnu standardizaciju transakcija. Isto važi i za zaštitu od platnih provajdera. Zamena za takvu nedostižnu anonimnost već postoji – odgovornost drugog učesnika

u transakciji i platnog provajdera: "Jednostavno, da se podaci iz moje evidencije plaćanja ne iskorišćavaju na moju štetu" (ibid). Ako je ova odgovornost zakonski sankcionisana, treća lica i entiteti ne bi smeli da imaju neovlašćeni pristup podacima o transakcijama. U tom slučaju se pokazuje da anonimnost plaćanja nije uslov za privatnost transaktora.

Otuda je razumljivo zašto je rašireno mišljenje da samo gotovinsko plaćanje osigurava privatnost. Koren ove predrasude je ubeđenje da su sve gotovinske transakcije nedokumentovane. Naprotiv, brojne uplate gotovine u prošlosti, a i danas, službeno su ili neslužbeno dokumentovane, što znači da nisu anonimne.

Danas većina pojedinačnih transaktora ne razmišlja o svojoj privatnosti i ne smatra da je *anonimnost bitna.* Sva prethodna razmatranja potvrdila su da je suština u privatnosti, a ne u anonimnosti. U poređenju sa praktično utopističkom i zakonski zabranjenom *potpunom nesledljivošću,* realna opcija je *čvrst stav o privatnosti,* kako za pojedince, tako i za firme i institucije. "Privatnost se odnosi na to koliko detalja entiteti sistema znaju o korisničkim transakcijama. Takođe pokriva koliko jedna institucija zna o podacima drugih institucija. Čvrst stav o privatnosti znači da su korisnički podaci vidljivi samo korisniku i onoliko institucija koliko je neophodno" (Darbha, str. 9).

Nesporno je da neanonimnost transakcija u postojećem regulatornom sistemu nije pretnja privatnosti transaktora i postavlja se pitanje u čemu je problem. Šta stalno narušava privatnost transaktora otkrivajući njihove transakcijske i finansijske podatke trećim licima? Odgovor je očigledan: nekontrolisana i neovlašćena prodaja svih ličnih podataka pod obmanjujućim nazivom *deljenje podataka (data sharing).*

*Šta je rešenje: anonimnost ili regulacija deljenja podataka*

Istraživanje prikazano u prethodnim odjeljcima pokazuje da anonimnost plaćanja nikada nije bila zaštita transaktora, isključujući sitne maloprodajne transakcije u gotovini. Uprkos ovom milenijumskom iskustvu, veličanje anonimnosti plaćanja sigurno će se nastaviti i narednih godina, a možda i decenija. Dovoljno je navesti obećanja kripto inovatora o *nesledljivosti* i *nepovezanosti* transakcija kao rešenja za privatnost transaktora. Potrebno je razotkriti fikciju anonimnosti.

Svaka ekonomska transakcija uključuje najmanje dve strane (prodavca i kupca) i nezaobilaznog posrednika u platnom prometu (pružalac usluga platnog prometa). Sve ove transakcije podrazumevaju dokaze o uplatama i dokumentaciju, osim u slučajevima svakodnevnih malih uplata. To je nerešiv problem za svaki pokušaj postizanja anonimnosti plaćanja tehnološkim inovacijama poput kriptovaluta. Jednostavno, druga ugovorna strana mora znati ko je izvršio uplatu (identifikacijski podaci), iznos, datum i za koju namenu (podaci o transakciji). Druga strana ne mora znati vaš broj računa ili naziv vaše banke, ali vaš platni provajder mora znati ove i druge povezane ID i podatke o transakciji. Ne postoje algoritamske tehnike kojima bi se zaobišla ili izbegla takva dvostrana konstrukcija, čak i ako se plaćanja u nekoj neodređenoj budućnosti počnu vršiti direktno, sa jednog računa na drugi. Čak i ako je posrednik na neki način hipotetički

eliminisan, druga strana u transakciji ne može biti eliminisana. Ovaj detalj ostao je nevidljiv svim kripto dizajnerima, počevši od Nakamota.

Alternativa utopističkoj anonimnosti plaćanja je regulacija deljenja podataka, koja se nameće kao najefektivnije rešenje zaštite privatnosti transaktora. Takvo rešenje podrazumeva regulisanje pristupa i obrade podataka o plaćanju. Ograničenje pristupa informacijama i dalje je dobra metoda zaštite privatnosti koju banke koriste vekovima. Zahvaljujući ovoj jednostavnoj metodi, banke su najuspešnije u zaštiti privatnosti transakcija, što je razlog zašto većina ljudi prihvata deljenje podataka samo sa svojim bankama (oko 85% prema prethodno navedenim istraživanjima).

Dizajner Bitcoina je kritikovao ovaj način postizanja anonimnosti u bankarstvu i bilo kakvu uključenost *treće strane od poverenja* u transakcije (Nakamoto, str. 6). Ovo je netačno, kao što je objašnjeno na početku ovog odeljka, ali je korisno za kriptografsku podršku fikciji o anonimnosti plaćanja. Pravnom implementacijom Nakamotovih sugestija u PSD2 pravilima i *Open Banking* inicijativi izvršena je *deregulacija dijeljenja podataka* pod političkim sloganom liberalizacije tržišta platnih usluga i njegovog potpunog otvaranja za inovativne *fintech* i *bigtech* konkurente.

Bigtech IT monopoli koriste slabosti postojeće regulative zaštite privatnosti, zasnovane na *obaveštenju* i *izboru korisnika.* "Izbor korisnika" postao je način da industrija prebaci krivicu na korisnike" (Abelson, 2013.).

Isto važi i za *pristanak potrošača* u PSD2 i otvorenom bankarstvu. Potrošači po pravilu ne znaju tačno ili ne razumeju na šta se njihov pristanak odnosi. Još gore, banke ne znaju tačno našta su njihovi klijenti pristali. Prvo, da li je to pristup treće strane svim platnim transakcijama ili stanju na računu? Drugo, kakva je veza između autentifikacije i pristanka potrošača? Šta je tačno *izričit* pristanak potrošača za PSD2? I na kraju, šta se događa sa prikupljenim podacima o plaćanju potrošača

Uprkos postojanju brojnih pravila i zakona koji određuju kako se podaci o plaćanju koriste i dele, kao i razvijenoj *tehnologiji za podršku informacionoj odgovornosti* (Abelson, 2013.), privatnost transakcija postaje sve ugroženija. Primarni uzrok ovakvog trenda je liberalizacija regulatornog okvira deljenja podataka, koja se razotkriva kao radikalna deregulacija. Očigledni primeri su revidirana Direktiva o platnim uslugama (PSD2) i inicijativa Otvoreno bankarstvo, čije se sprovođenje zaglavilo između nepoverenja većine transaktora i opstruktivnih tehničkih standarda banaka (API standardi za deljenje podataka). Regulatorno navođenje potrošača da se udalje od svojih pouzdanih platnih provajdera i prisiljavanje banaka na deljenje podataka ugrožavaju privatnost transaktora.

*Prvi put objavljeno na* https://centralbankmoneyresearch.com/