Mešanje poverljivih transakcija: Sveobuhvatna privatnost Bitcoin transakcija

Seminarski rad u okviru kursa
Kriptografija
Matematički fakultet

Miloš Samardžija
mi13304@alas.matf.bg.ac.rs

29. maj 2017

Sažetak

Ovaj tekst predstavlja sažetak rada *Mixing Confidential Transactions: Comprehensive Transaction Privacy for Bitcoin* [1]. Ukratko su prikazani problemi sa privatnošću Bitcoin transakcija, njihova delimična rešenja, poteškoće sa kompatibilnošću koje se javljaju prilikom spajanja ovih rešenja, i sam protokol ValllueShuffle koji ih prevazilazi. Opisani su gradivni blokovi ovog protokola, kao i neke od njegovih karakteristika.

Sadržaj

1 Uvod

U inicijalnom dizajnu Bitcoina, privatnost igra samo sporednu ulogu. Prvobitno mišljenje da Bitcoin pruža anonimnost je odbačeno od strane mnogih akademskih radova koji pokazuju brojne slabosti koje se tiču privatnosti tekućeg protokola. Javna priroda distribuirane baze podataka Bitcoin transakcija (eng. blockchain) je ta koja se pokazala nebezbednom za privatnost korisnika. Ovo je prouzrokovalo razvoj mnogobrojnih tehnologija koje pospešuju privatnost u cilju prevazilaženja uočenih nedostataka, bez menjanja fundamentalnog dizajna Bitcoina.

Ipak, postojeća rešenja nude samo delimična rešenja, koja se fokusiraju samo na jedan aspekt privatnosti (anonimnost isplatioca, anonimnost primaoca ili anonimnost vrednosti isplate). Npr. poverljive transakcije (eng. Confidential Transactions) su predloženo unapređenje protokola koje definiše takav format transakcije koji omogućava anonimnost vrednosti isplate u bazi transakcija. Tajne adrese (eng. Stealth Addresses) su mehanizam koji isplatiocima omogućava da generišu jedinstvene privremene adrese kako bi se poboljšala privatnost primaoca sredstava. Kada je u pitanju privatnost isplatioca, preovlađujući pristup koji je kompatibilan sa Bitcoinom je mešanje novčića (eng. coin mixing). Takva funkcionalnost se u praksi ostvaruje spajanjem više transakcija u jednu, generisanjem Bitcoin transakcije sa više ulaza i više izlaza, čime se prikriva veza između novčanih sredstava i njihovih vlasnika. Svaki učesnik u transakciji mora da je potpiše kako bi ona bila validna, čime se sprečava krađa sredstava.

Da bi se postigla sveobuhvatna privatnost, potrebno je kombinovati sva tri delimična rešenja u jedno. Međutim, kombinovanje poverljivih transakcija sa P2P mešanjem novčića predstavlja izazov.

2 ValueShuffle: Mešanje poverljivih transakcija

ValueShuffle predstavlja prvi protokol mešanja novčića koji je kompatibilan sa poverljivim transakcijama. Predstavlja nadogradnju P2P protokola za mešanje novčića - CoinShuffle++. S obzirom da ValueShuffle uspešno kombinuje sva rešenja, rezultujuća valuta pruža sveobuhvatnu privatnost, tj. anonimnost isplatioca, anonimnost primaoca i anonimnost vrednosti isplate. S obzirom da se oslanja na CoinJoin, protokol nasleđuje razne karakteristike ključne za praktičnu primenu u Bitcoin ekosistemu, npr. Bitcoin skriptove i kompatibilnost sa blockchain potkresivanjem (eng. blockchain pruning). Gradivni blokovi protokola su P2P mešanje, poverljive transakcije i tajne adrese.

Iskorišćavanje sinergija. Kombinovanjem mehanizma mešanja novčića sa tajnim adresama i poverljivim transakcijama, iskorišćavamo važne sinergije koje P2P mešanje novčića čini efikasnijim i praktičnijim. To ostvarujemo prevazilaženjem dva glavna nedostatka postojećih rešenja.

Prvi nedostatak je taj što mešanje novčića zahteva da vrednosti sredstava koja se šalju budu ista za sve učesnike u transakciji, jer bi u suprotnom bilo trivijalno pronaći vezu između ulaza i izlaza iz transakcije. Dodavanjem anonimnosti vrednosti isplate, uklanja se ovo ograničenje, ali se onda postavlja pitanje kako dokazati da vrednost izlaza transakcije ne prevazilazi vrednost ulaza, čime bi se novac stvorio ni iz čega.

Drugi nedostatak je taj što mehanizam zahteva od korisnika da sredstva prvo pošalje na sveže generisanu adresu, čime se uklanja bilo kakav

trag o vlasniku sredstava. Tek nakon toga, u drugoj transakciji, sredstva se šalju primaocima.

Dakle, privatnost ima veliku cenu, s obzirom da se generiše duplo više transakcija nego što je zaista potrebno. Ovo posebno ima negativan uticaj na korisnike koji plaćaju dodatne takse i moraju da čekaju duže. Kod ValueShuffle protokola, oslanjamo se na na mehanizme tajnih adresa i poverljivih transakcija kako bismo sredstva poslali direktno očekivanim primaocima.

2.1 Karakteristike protokola

Sveobuhvatna privatnost. ValueShuffle osigurava da napadač koji nadgleda blockchain ili mrežu, ili čak učestvuje u protokolu ne može da pronađe vezu između ulaza i izlaza transakcije. Dodatno, tajne adrese pružaju kratkoročne adrese za primanje sredstava, čime se postiže anonimnost primaoca, i poverljive transakcije pružaju anonimnost vrednosti sredstava.

Jedna transakcija. Protokol se koristi tako da se sredstva direktno šalju namenjenim primaocima. Kao rezultat, privatna plaćanja mogu biti izvršena samo jednom transakcijom u blockchainu.

Otpornost na DoS napade. Zlonamerni korisnici mogu da izazovu zakašnjenja u protokolu, ali ga ne mogu sprečiti. Pošto je ValueShuffle zasnovan na efikasnom CoinShuffle++ protokolu, uspešno se završava u samo 4 + 2f komunikacionih rundi, u prisustvu f zlonamernih korisnika.

Anonimni kanal nije obavezan. Za pružanje nepovezivosti između ulaza i izlaza, protokol ne koristi anonimne kanale poput Tor mreže. Ipak, napadač bi ulazne adrese mogao da poveže sa mrežnim identifikatorom, poput IP adrese, pa se preporučuje upotreba anonimne komunikacije.

2.2 Karakteristike nasleđene iz CoinJoin

Pošto je ValueShuffle zasnovan na CoinJoin paradigmi, dodatno nasleđuje sve njene prednosti:

- **Otpornost na krađu** - S obzirom da korisnici proveravaju konačnu CoinJoin transakciju pre potpisivanja, novac ne može biti ukraden.
- **Kompatibilnost sa skriptovima** - Pošto u protokolu skripte nisu poverljive, kompatibilan je sa izlazima transakcija koji koriste kompleksne skripte.
- **Smanjeni troškovi i memorijsko zauzeće** - Uvođenjem Šnorovih potpisa, omogućava se korišćenje agregiranih potpisa, čime se umesto n potpisa koristi samo jedan, gde je n broj korisnika.
- **Podstiče privatnost** - Zbog smanjenih troškova, korisnici štede novac korišćenjem transakcija koje obezbeđuju privatnost. To predstavlja odličan podsticaj za razvoj i upotrebu ovog protokola.
- **Kompatibilnost sa potkresivanjem.** Potkresivanje smanjuje probleme sa skaliranjem Bitcoin protokola.

2.3 Pregled protokola

Pretpostavimo da se svaki korisnik i predstavlja trojkom $in_i = (c_i = Com(x_i, r_i), \pi_i)$, gde je c_i rezultat kriptografske funkcije (eng. additively

homomorphic commitments) koja omogućava dokazivanje da vrednost izlaza transakcije ne prevazilazi vrednost ulaza, bez samog otkrivanja vrednosti sredstava, x_i je vrednost ulaznih sredstava, r_i je nasumična vrednost, π_i (eng. range proof) je vrednost pomoću koje se osigurava da vrednost sredstava nije negativna ili previše velika, i vk_i je Bitcoin adresa korisnika i.

Apstraktno posmatrano, izvršavanje protokola se sastoji od pokretanja (eng. runs), i svako pokretanje se sastoji od 4 faze:

- **Generisanje izlaza.** Svaki korisnik i lokalno generiše trojku $out_i = (c_i', \pi_i', addr_i')$, gde je c_i' kriptovana vrednost sredstava, π_i' je odgovarajući range proof, i $addr_i'$ je sveže generisana kratkoročna adresa primaoca. Primetimo da korisnici mogu imati više izlaznih trojki, ali radi jednostavnosti, fokusiraćemo se na slučaj kada postoji samo jedna.
- **Mešanje i sigurno sabiranje.** Korisnici paralelno izvršavaju P2P protokol kako bi izračunali njihove izlazne trojke out_i i kako bi poverljivo izračunali sumu $r_\Delta = \sum_i r_i' - r_i$. Konačno, ulazne i izlazne poruke mogu biti kombinovane kako bi se kreirala CoinJoin transakcija dodavanjem nasumične vrednosti r_Δ.
- **Provera.** Korisnici proveravaju validnost rezultujuće transakcije, tj. proveravaju da li sve vrednosti π_i' odgovaraju vrednostima c_i', i proveravaju da li je ukupan bilans korektan. Takođe, svaki korisnik proverava da li je odgovarajuća izlazna trojka deo rezultata mešanja, tj. da nije došlo do krađe novca u transakciji.
- **Potvrđivanje ili okrivljivanje.**
  - **Potvrđivanje.** Ako sve provere prođu, transakcija je validna i od korisnika se zahteva da je potpišu. Iako svaki korisnik proverava samo da li je njegov izlaz validan, algoritam DiceMix garantuje da je to dovoljno da se dokaže da su izlazi svih korisnika validni. Dakle, ukoliko je neki korisnik došao do ove tačke, može biti siguran da su korisnici koji odbijaju da potpišu transakciju zlonamerni. Ako se to dogodi, takvi korisnici se isključuju i vrši se novo pokretanje protokola.
  - **Okrivljivanje.** Ukoliko rezultat neke od gore pomenutih provera bude negativan, pokreće se ova faza kako bi se detektovao bar jedan zlonameran korisnik. Svaki korisnik i emituje nasumični broj koji je koristio za protokole mešanja i sigurne sume, čime otkriva vrednost $r_i - r_i'$, što je dovoljno da se proveri da je korisnik i koristio istu vrednost sredstava u ulaznim i izlaznim adresama (i da na taj način nije kreiran novac ni iz čega). Sada svaki korisnik j može da ponovi korake mešanja i sigurne sume korisnika i, i da proveri da li je korisnik i poštovao protokol. Nakon toga, zlonamerni korisnik se isključuje iz protokola, i vrši se novo pokretanje.

2.4 Bezbednost i privatnost

ValueShuffle pruža sledeće garancije u pogledu sigurnosti i privatnosti:

- **Nepovezivost.** Za dati izlaz, i dva ulaza u CoinJoin transakciji, napadač ne može da proceni koja od ulaznih adresa odgovara izlaznoj.
- **Kompatibilnost sa poverljivim transakcijama.**

- **Otpornost na krađu.** Sredstva svakog korisnika se ili prebacuju primaocu kome su namenjena, ili ostaju u posedu prvobitnog vlasnika.
- **Uspešno zaustavljanje.** Protokol se zaustavlja uspešno za korisnike koji ga poštuju.

Literatura

[1] Tim Ruffing and Pedro Moreno-Sanchez. Mixing Confidential Transactions: Comprehensive Transaction Privacy for Bitcoin, 2017. on-line at: http://eprint.iacr.org/2017/238.pdf.