**Vodič za sigurnost kriptovaluta**

Kriptovalute su promijenile način na koji ljudi obavljaju digitalne transakcije. U kripto transakcijama se ne razmjenjuje materijalni novac. Umjesto toga, finansijske transakcije se odvijaju kao digitalni unosi u online bazu podataka koji identifikuju specifične transakcije. Transakcije kriptovalutama su brže i sigurnije, omogućavajući korisnicima da obavljaju transakcije bez potrebe posredničke finansijske institucije kao što je banka.

Ali, da li je kriptovaluta sigurna? Rastuća popularnost kriptovaluta učinila je kripto kompanije, berze i novčanike privlačnom metom za sajber kriminalce. Kao rezultat toga, veći je naglasak na podizanju kibernetičke sigurnosti kriptovalute kako bi se osigurala zaštita povezanih platformi i upotrebe.

U ovom sigurnosnom vodiču za kriptovalute detaljno ćemo pogledati važnost sigurnosti u kriptovaluti, koja je kriptovaluta najsigurnija, uobičajena sigurnosna pitanja kriptovalute i kako osigurati kriptovalutu.

**Šta je kriptovaluta?**

Kriptovaluta je digitalna valuta, zasnovana na blockchain tehnologiji, koja korisnicima omogućava sigurna digitalna plaćanja putem tokena. Najčešće kriptovalute koje se danas koriste su: Bitcoin, Litecoin, Ethereum, Monero, Binance Coin i tako dalje.

Transakcije kriptovaluta su brze i rade na decentralizovanim mrežama koje su nezavisne od bilo kakve državne kontrole. Burze kriptovaluta olakšavaju kupovinu, trgovanje i ulaganje u kriptovalute.

**Šta je sigurnost kriptovaluta?**

Mjere koje se poduzimaju za osiguranje kripto transakcija od prijevarnih aktivnosti i održavanje sigurnosti digitalne valute nazivaju se sigurnost kriptovaluta. Osim što zahtijevaju korisničko ime i verifikacijski kod za prvu upotrebu, kripto berze koriste tehnike blockchaina i kriptografije kako bi poboljšale kripto sajber sigurnost, učinile transakcije sigurnijim i zaustavile prijevare s kriptovalutama.

Transakcije kriptovalutama su digitalne prirode i prate složeni backend proces. Tehnologija koja stoji iza sigurnosti kriptovalute je blockchain koji je u suštini distribuirana baza podataka ili knjiga koja se dijeli između brojnih čvorova računalne mreže. Blockchain pruža sveobuhvatno upravljanje rizikom od sajber prijetnji koristeći okvire kibernetičke sigurnosti i najbolje prakse. Kriptografija štiti informacije i komunikaciju i koristi kodove kako bi osigurala da ih mogu koristiti samo ovlaštene osobe.

**Koja kriptovaluta je najsigurnija?**

Ethereum se smatra najsigurnijom kriptovalutom u odnosu na drugu digitalnu imovinu. To je uglavnom zato što njegova platforma koristi blockchain tehnologiju, koja je jedna od najrobusnijih tehnologija za digitalne transakcije.

Nadalje, kako bi poboljšao sigurnost platforme, Ethereum koristi metodu konsenzusa dokaza o udjelu, koja odvraća loše aktere tako što ne pruža nikakva sredstva za iskorištavanje ili kontrolu mreže.

**Uobičajeni sigurnosni problemi kriptovalute**

Posljednjih godina kriptovalute su postale sve popularnije, a koristi ih veliki broj potrošača. Ova rastuća popularnost privukla je pažnju loših aktera, koji se upuštaju u brojne prevare i prijevarne aktivnosti.

Prijevarne mogućnosti ulaganja, nelegitimne kripto platforme, sigurnosni rizici za rudarenje kriptovaluta, lažni novčanici i tako dalje neki su od najčešćih oblika sigurnosnih problema kriptovaluta koji prevladavaju u segmentu kriptovaluta. Pogledajmo pobliže neke od problema u svijetu kriptovaluta:

* *Phishing*: Loši akteri kreiraju lažne web stranice ili šalju e-poštu predstavljajući se kao legitimne mjenjačnice kriptovaluta ili provajderi novčanika kako bi prevarili korisnike da podijele svoje vjerodajnice za prijavu, izvorne riječi ili privatne ključeve. Ponekad klikanje na link može dovesti do sigurnosnih rizika za rudarenje kriptovaluta. Ovdje se kod za rudarenje kriptovalute može učitati na računare korisnika, rudareći kriptovalutu za napadača, dok žrtva može vidjeti samo kako se njihovi računari usporavaju.
* *Ponzi šeme*: sajber kriminalci koriste lažne šeme u kojima obećavaju visok povrat ulaganja i oslanjaju se na sredstva novih investitora da bi isplatili ranije investitore. Na kraju, u nedostatku dovoljno novih investitora da održe šemu, ona propada.
* *Lažne početne ponude kovanica (ICO)*: Pokretanjem lažnih ICO-a, nuđenjem novih tokena ili kovanica u zamjenu za ulaganja, loši akteri prevare nesuđene korisnike. Napadači kreiraju web stranice profesionalnog izgleda kako bi privukli investitore i nestali čim prikupe sredstva.
* *Pump and Dump sheme*: U ovoj prevari, loši akteri umjetno naduvaju cijenu kriptovalute male količine putem lažnih ili obmanjujućih informacija. Zatim ga prodaju na vrhuncu kako bi ostvarili profit, uzrokujući značajne gubitke investitorima. Često napadači formiraju grupe u aplikacijama za razmjenu poruka i na platformama društvenih medija kako bi izvršili ove šeme.
* *Lažni novčanici i razmjene*: Kreiranjem zlonamjernih novčanika ili razmjena koje izgledaju istinski, loši akteri kradu korisnička sredstva ili lične podatke. Oni oglašavaju svoje lažne novčanike na popularnim pretraživačima i platformama društvenih medija kako bi stekli privlačnost. Ako korisnik klikne na oglas
* *Prevare s poklonima na društvenim mrežama*: U ovoj vrsti prijevare, sajber kriminalci se imitiraju kao istaknute javne ličnosti na platformama društvenih medija i obećavaju da će pokloniti kriptovalute. Da bi dobili besplatne, korisnici moraju poslati naknadu za pokriće u kriptovaluti ili da potvrde svoj identitet. Međutim, obećana nagradna igra se nikada ne dešava.
* *Napadi zlonamjernog softvera i ransomwarea*: Ovo je metoda za dobivanje pristupa računalima ili mobilnim uređajima korisnika postavljanjem zlonamjernog softvera, a zatim krađom njihove kriptovalute ili šifriranjem njihovih podataka i traženjem otkupnine za njihovo oslobađanje.
* *Napadi dvostruke potrošnje*: Ovdje napadač može potrošiti vlastitu kriptovalutu i zatim izbrisati transakciju.

**Kako je kriptovaluta sigurna?**

Ako centralizirane mreže imaju sigurnosni propust, napadači mogu pristupiti korisničkom računu. Međutim, gotovo je nemoguće da napadač hakuje kripto mrežu koja je decentralizirana. To je zato što napadači ne mogu ukrasti korisnikovu kriptu bez pristupa njihovom privatnom ključu.

Glavni razlozi zašto je teško narušiti sajber sigurnost u kriptovaluti su navedeni u nastavku:

* *Stanje*: Nekoliko čvorova na mreži kriptovaluta ima kopiju baze podataka. U slučaju, napadač je uspješan u promjeni ravnoteže na jednom čvoru, on će se razlikovati od balansa na drugim čvorovima. Ovo stvara anomaliju koja rezultira odbacivanjem ravnoteže prikazane u kompromitovanom čvoru.
* *Potpisi*: Važeći potpisi su preduvjet za svaku transakciju. Ako čvor odobri transakciju, i ostali čvorovi bi trebali potpis da bi proglasili transakciju validnom. Međutim, ako se potpis ne proizvede, drugi čvorovi će odbiti transakciju.
* *Zaštita*: Kripto sigurnost zabranjuje napade dvostruke potrošnje, koji uključuju kompromitaciju čvora koji mora prikazati povijest transakcija dužu od svih ostalih čvorova, čineći ove napade skupim investicijama, često daleko nadmašujući potencijalne povrate.

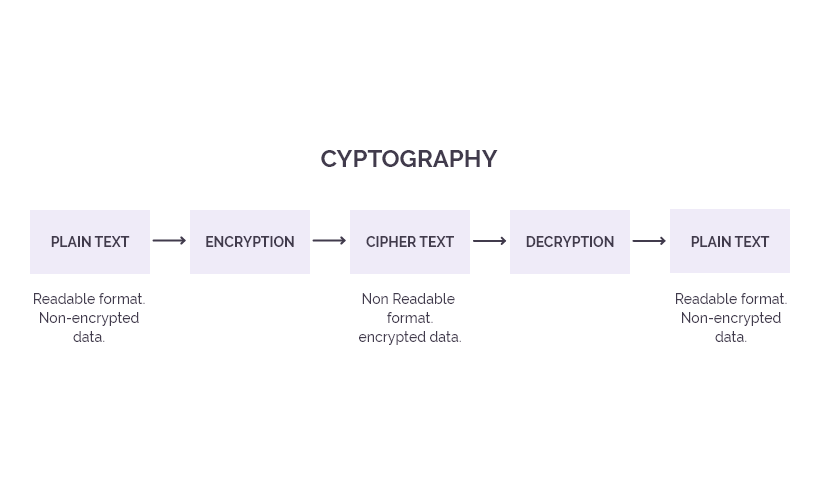
**Koji su sigurnosni standardi kriptovaluta?**

Zahtjevi specificirani za korištenje sistema kriptovaluta, uključujući burze kriptovaluta, mobilne i web aplikacije, zajednički se nazivaju Standardi sigurnosti kriptovaluta. Ovi standardi pomažu u upravljanju i standardizaciji tehnika, kao i poboljšanju sigurnosti kriptovaluta.

Postoji deset ključnih tačaka navedenih u Standardima sigurnosti kriptovaluta (CCSS) koje većina berzi kriptovaluta koristi prilikom postavljanja sigurnosnih sistema kriptovaluta. Ključni koraci usklađeni sa sigurnosnim standardima kriptovalute uključuju: generiranje ključeva/seeda, kreiranje novčanika, pohranu ključeva, korištenje ključeva, politiku kompromisa s ključevima, politiku i procedure dodjele/povlačenja ključeva, revizije trećih strana, politiku sanacije podataka, dokaz o rezervi, i revizije dnevnika.

**Kako kriptografija poboljšava sigurnost kriptovalute?**

Kriptografija je tehnika koja pomaže u zaštiti kriptovalute osiguravanjem informacija i komunikacije autentifikacijom transakcije. Prilikom kreiranja novčanika, generira se "hash" jedinstven za taj novčanik.



Tokom transakcije, heš se prenosi sa šifrovanim informacijama o adresi primaoca i iznosu koji se prenosi. Takođe je potpisan privatnim ključem pošiljaoca. Za završetak transakcije, ne samo da primalac mora dati javni ključ koji je generirao novčanik pošiljaoca, već se moraju poklapati i sve ostale informacije.

**Načini poboljšanja kripto sigurnosti**

Kriptovalute imaju ogromnu novčanu vrijednost, što ih čini privlačnim za napadače. Kao što je ranije objašnjeno, postoji mnogo načina na koje napadači mogu ciljati sigurnosne sisteme kriptovaluta.

Kako bi spriječili napadače da iskorištavaju njihove platforme, uzrokuju gubitke i ometaju digitalno iskustvo pravih korisnika, kompanije za kriptovalute moraju razmotriti načine za jačanje sajber sigurnosti kriptovaluta. Moraju poduzeti proaktivne mjere kako bi osigurali sigurnost svojih platformi i računa svojih klijenata. Evo nekoliko koraka koje bi mogli razmotriti implementaciju:

* *Procjena rizika*: Od ključne je važnosti provesti detaljnu procjenu rizika kako bi se identificirale potencijalne ranjivosti, prijetnje i rizici specifični za poslovanje s kriptovalutama, kao i da bi se odredili prioriteti napori za ublažavanje.
* *Zaštita privatnog ključa*: Kriptovalute koriste kriptografske ključeve, posebno privatne ključeve, za pristup i kontrolu vlasništva nad digitalnom imovinom. Zaštitite privatne ključeve pomoću tehnika kao što su enkripcija, sigurno skladištenje i hardverski novčanici.
* *Sigurnost novčanika*: Jake lozinke, višefaktorska autentifikacija (MFA) i redovna ažuriranja softvera novčanika su ključni za poboljšanje sigurnosti novčanika.
* *Dvofaktorska autentifikacija*: implementirajte 2FA da dodate dodatni sloj sigurnosti na račune kriptovaluta.
* *Sigurne transakcije*: Provjerite adresu novčanika primatelja koristeći dodatne sigurnosne funkcije kao što su potpisivanje transakcija i šifriranje.
* *Mrežna sigurnost*: Koristite kriptografske algoritme i nadgledanje mreže kako biste zaštitili infrastrukturu blockchaina od napada vođenih botovima, kao što su napadi distribuiranog uskraćivanja usluge (DDoS). Implementirajte zaštitne zidove, sisteme za otkrivanje i prevenciju upada (IDPS) i virtuelne privatne mreže (VPN), jaku enkripciju i redovno zakrpe i ažuriranje mrežnih uređaja.
* *Crypto Exchange sigurnost*: Exchange sigurnost uključuje mjere za zaštitu korisničkih naloga, sigurno skladištenje imovine, autentifikaciju u dva faktora (2FA), procedure protiv pranja novca (AML) i poznavanja svog klijenta (KYC), redovne revizije sigurnosti i pridržavanje prema regulatornim standardima. Omogućite dodatne sigurnosne funkcije kao što su bijele liste za povlačenje ili IP ograničenja i prakticirajte dužnu pažnju prilikom odabira trgovinskih partnera.
* *Šifriranje podataka*: Šifrirajte osjetljive podatke, kako u prijenosu tako i u mirovanju, koristeći nekoliko dostupnih tehnika šifriranja kako biste podatke zaštitili od neovlaštenog pristupa ili presretanja.
* *Sigurnost pametnog ugovora i tokena*: slijedite sigurne prakse kodiranja i osigurajte odgovarajuće testiranje prije implementacije.
* *Jake prakse lozinki*: Dajte smjernice za kreiranje robusnih lozinki i preporučite korištenje upravitelja lozinki za sigurno pohranjivanje i upravljanje vjerodajnicama.
* *Kontrola pristupa i korisničke privilegije*: Implementirajte jake kontrole pristupa i korisničke privilegije kako biste ograničili pristup osjetljivim podacima i sistemima.
* *Ažuriranja softvera i firmvera*: Redovno ažurirajte novčanike za kriptovalute, softverske klijente i firmver za hardverske novčanike, jer ova ažuriranja mogu sadržavati sigurnosne zakrpe i poboljšanja za poboljšanu zaštitu od poznatih prijetnji.
* *Sigurnosna kopija i oporavak*: Redovno pravite sigurnosnu kopiju novčanika kriptovaluta i sigurno čuvajte sigurnosnu kopiju.

**Reference**

1. *ArkoseLab*, (2022, Mart) Guide to cryptocurrency security  
   <https://www.arkoselabs.com/explained/guide-to-cryptocurrency-security/>
2. *Steven Ehrlich, Forbes* (8. mart 2023.) Crypto Security: A Beginner’s Guide <https://www.forbes.com/sites/digital-assets/article/crypto-security-overview/?sh=5f69cac384c1>