

# **SIGURNOST CRYPTO WALLET-A**

**IVANOVIĆ ANTONIO 4.RT**



# ŠTO JE CRYPTO WALLET?

- Fizički medij, program, internetska usluga
- Sadrži javne/privatne ključeve
- Nudi kriptiranje ili potpisivanje informacija

# VRSTE CRYPTO WALLET-A

- Vrste:
  - Softverski novčanici
    - Full client
    - Lightweight client
    - Web novčanici
  - Hladni novčanik
    - Papirnati novčanik
    - Hardverski novčanici

# HOT WALLET VS. COLD WALLET

- Hot wallet
  - Day-to-day transakcije
  - Veća ranjivost internet napadima
- Cold wallet
  - Velike količine kriptovaluta
  - Fizička šteta



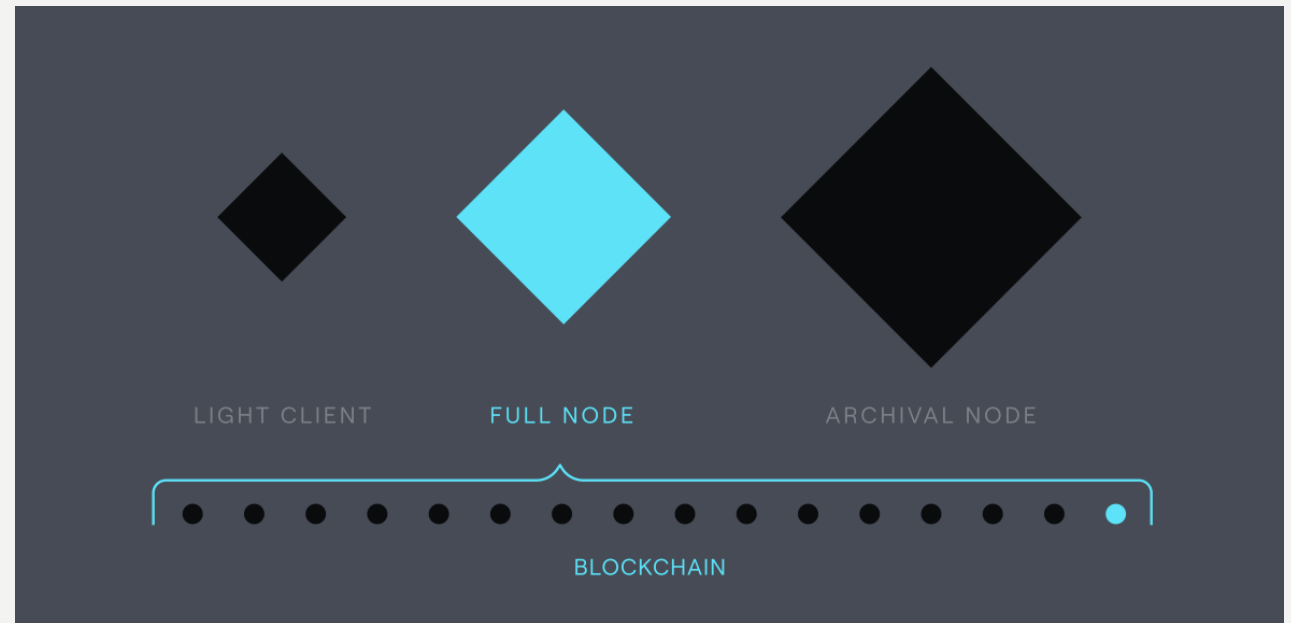
# **SOFTWARE WALLET**

- Potpuni klijent
- Lagani klijent
- Web wallet
  - Jednostavnost
  - Povjerenje u poslužitelja
- MetaMask, Coinbase wallet, Trust wallet

# SOFTVERSKI NOVČANICI

## FULL CLIENT

- Preuzima kopiju blockchaina
- Provjerava valjanost transakcije
- Sprječava minanje blokova koji krše ili mijenjanju mrežna pravila



# SOFTVERSKI NOVČANICI

## LIGHTWEIGHT CLIENT

- Oslanja se na pune čvorove u blockchainu
- Rizik od manipulacije
- Potencijalni gubitak sredstva



# **COLD WALLET**

- Fizički uređaj
- Radi izvan mrežnog okruženja
- Dodatni sloj sigurnosti



# HARDWARE WALLET

- Ledger Nano S, Trezor, KeepKey
- Pohranjuje privatne ključeve izvan interneta
- Smanjeni rizik od hakiranja



# PAPER WALLET

- Zapisivanje privatnog ključa na papir
- Fizički pohranjen na sigurnom mjestu
- Metalni novčanik



# Kako osigurati crypto wallet

- Koristiti 2FA
- Jedinstvene lozinke
- Ažuriranje software-a novčanika
- Prepoznati phishing napade i prevare




# Kako osigurati crypto wallet

- Napraviti backup podataka od crypto wallet-a
- Secret recovery ili mnemonic phrases
- Seed phrases



# SECRET RECOVERY

- Fraze čitljive ljudima
- Predstavljaju privatni ključ wallet-a
- Software generira fraze

 METAMASK

[< Back](#)

## Confirm your Secret Recovery Phrase

Please select each phrase in order to make sure it is correct.

surprise	that	true	local
promote	amateur	stage	neck
acoustic	order	tilt	puppy

acoustic	amateur	local	neck
order	promote	puppy	stage
surprise	that	tilt	true

# SEED PHRASES

- **Koriste se uz secret recovery fraze**
- **Generirane sa standardnim algoritmom**
- **Kompaktibilne na više wallet-a**



METAMASK

## Secret Backup Phrase

Your secret backup phrase makes it easy to back up and restore your account.

**WARNING:** Never disclose your backup phrase. Anyone with this phrase can take your Ether forever.

inside rug engine permit peer  
squeeze slight aspect sudden traffic  
crash giraffe

Remind me later

Next

# Principi dobre prakse

- Zapisati frazu na papir
- Više kopija fraze
- Ne dijeliti fraze drugim ljudima
- Metal backup
- Kriptiranje podataka





# ČESTE PREVARE

- Promocija junk tokena
- Rug pull
- Prevarantno ulaganje
- Poruke preko društvenih mreža





# PRIMJER WALLET ADRESA

- 1Lbcfr7sAHTD9CgdQo3HTMTkV8LK4ZnX71
- Primjer **Bitcoin** wallet adrese
- able caution health style use nature verb  
already winner gesture verb
- Primjer **privatnog** ključa

BOB



Servers



ALICE



# PITANJA ZA PONAVLJANJE

- 1. Što je to crypto wallet?
- 2. Koje su vrste crypto wallet-a?
- 3. Kakva je razlika između hot i cold wallets?
- 4. Kako osigurati crypto wallet?
- 5. Što je Secret Recovery i kako se koristi za sigurnost crypto walleta?

# PITANJA ZA PONAVLJANJE

- 1. Crypto wallet je fizički medij, program ili internetska usluga koji sadrži javne/privatne ključeve, te pruža kriptiranje ili potpisivanje informacija radi dodatne sigurnosti.
- 2. Postoje softverski novčanici (full client, lightweight client, web novčanici) i hladni novčanici (papirnati, hardverski novčanici).
- 3. Hot wallets su lakši za svakodnevno korištenje i pristupačni korisnicima, dok cold wallets pružaju bolju sigurnost za dugoročno pohranjivanje većih količina kriptovaluta.
- 4. Osiguravanje crypto walleta uključuje upotrebu 2FA, snažnih lozinki, redovnog ažuriranja softvera, prepoznavanje phishing napada, izradu backupa podataka te korištenje secret recovery ili mnemonic fraza.
- 5. Secret Recovery je mnemonična fraza koja predstavlja privatni ključ crypto walleta. Generira se od strane softvera i koristi se za povratak novčanika.