



FAKULTET TEHNIČKIH NAUKA
Informacione tehnologije
Informacione tehnologije

KRIPTOGRAFIJA I BLOKCHAIN
TEHNOLOGIJA

MAGISTARSKI RAD

Mentor:

Prof. dr Bogdan Mirković

Kandidat:

Ibrišimović Ermin

MIT-001/23

Brčko, novembar 2024. godine

Sadržaj

1. Uvod	5
1.1. Pozadina	5
1.2. Ciljevi rada	6
1.3. Metodologija istraživanja	7
1.4. Struktura rada.....	7
1.5. Hipoteze	8
2. Uvod u kriptografiju	10
2.1. Definicija kriptografije	10
2.2. Historija kriptografije.....	11
2.3. Kriptografski algoritmi i protokoli	13
2.3.1. Simetrična kriptografija	13
2.3.2. Asimetrična kriptografija	14
2.3.3. Hash funkcije	15
2.3.4. Digitalni potpisi.....	16
2.4. Kriptografija u očuvanju privatnosti na internetu.....	16
2.5. Kvantna kriptografija	17
2.5.1. Korekcija grešaka.....	19
2.5.2. Protokoli za verifikaciju	19
2.6. Kvantno otporna kriptografija	20
2.6.1. Prijetnje kvantnih računara	21
2.6.2. Ciljevi kvantno otporne kriptografije	21
2.6.3. Glavni matematički problemi u kvantno otpornim sistemima.....	21
2.6.4. Algoritmi kvantno otporne kriptografije	22
2.6.5. Izazovi kvantno otporne kriptografije	22
2.6.6. Primjena kvantno otporne kriptografije.....	22
2.7. Uticaj kriptografije na zakonodavstvo	23
2.7.1. Regulativa kriptografije	24
3. Uvod u Blockchain tehnologiju.....	25
3.1. Definicija blockchaina.....	25
3.2. Historija i razvoj blockchaina	26
3.3. Način rada blockchaina	27
3.3.1. Blokovi	27
3.3.2. Lanac.....	28
3.3.3. Rudarenje	29

3.4. Primjena blockchaina izvan kriptovaluta.....	30
3.5. Sigurnost blockchaina.....	30
3.5.1. Napadi na blockchain	31
3.5.2. Zaštita blockchaina	32
4. Blockchain i privatnost	33
4.1. Definicija privatnosti u kontekstu blockchaina	33
4.2. Mjere zaštite privatnosti u blockchainu	34
4.2.1. Anonimnost	34
4.2.2. Pseudonimnost.....	35
4.2.3. Zero-Knowledge dokazi	35
4.3. Izazovi očuvanja privatnosti na blockchainu	36
4.4. Pravna pitanja vezana uz privatnost na blockchainu	37
5. Primjena blockchain tehnologije u očuvanju privatnosti na internetu	38
5.1. Primjeri korištenja blockchaina za očuvanje privatnosti.....	38
5.2. Analiza postojećih rješenja	39
5.2.1. Bitcoin i privatnost	40
5.2.2. Ethereum i privatnost.....	40
5.2.3. Monero i privatnost.....	41
5.3. Prednosti i nedostaci korištenja blockchaina za očuvanje privatnosti.....	42
5.4. Prikaz alternativnih blockchain tehnologija za očuvanje privatnosti	43
5.4.1. Zcash i privatnost.....	44
5.4.2. Dash i privatnost.....	45
6. Studije slučaja.....	46
6.1. Studija slučaja: Primjena blockchaina u očuvanju privatnosti korisnika na internetu.....	46
6.1.1. Opis slučaja.....	46
6.1.2. Analiza rješenja.....	47
6.1.3. Procjena učinkovitosti	48
6.2. Studija slučaja: Implementacija blockchaina u lancu snabdijevanja – Walmart i IBM.....	49
6.2.1. Kontekst.....	49
6.2.2. Izazov	49
6.2.3. Rješenje	50
6.2.4. Rezultati.....	50
6.2.5. Osnovne karakteristike studije slučaja	50
6.3. Procjena primjenjivosti na druge sektore	51
6.3.1. Zdravstvena njega	51
6.3.2. Finansijski sektor	51

6.3.3. Online komunikacija	52
6.3.4. E-vladina rješenja	52
7. Budući razvoj i izazovi.....	52
7.1. Budući trendovi u blockchain tehnologiji	52
7.1.2. Razvoj decentraliziranih aplikacija (dApps)	56
7.1.3. Proširena privatnost i sigurnost	58
7.1.4. Regulatorna pitanja i standardizacija	60
7.2. Izazovi i ograničenja blockchain tehnologije	61
7.3. Moguća poboljšanja u očuvanju privatnosti korisnika na internetu	62
7.4. Tehnološka inovacija i utjecaj na privatnost i sigurnost.....	63
7.4.1. Poboljšanja u privatnosti i sigurnost	63
7.4.2. Izazovi u privatnosti i sigurnosti	63
7.4.3. Potreba za stalnim prilagodbama.....	64
7.5. Socijalni i etički izazovi povezani s blockchainom	64
7.5.1. Socijalna isključenost.....	64
7.5.2. Etički izazovi.....	64
7.5.3. Utjecaj na radna mjesta.....	65
7.5.4. Utjecaj na okoliš	65
8. Zaključak	65
9. Literatura	67