

CUPRINS

INTRODUCERE	9
1. BITCOIN: O PRIVIRE DE ANSAMBLU.....	11
1.1 Concepte de bază și definiții	11
1.1.1 Ce înseamnă de fapt Bitcoin?	11
1.1.2 Scurtă comparație între rolul Bitcoin, al băncilor și al altor sisteme de transfer de bani.....	17
1.1.3 Elementele defnitorii ale Bitcoin.....	20
2. ISTORIA LANȚULUI DE DATE (BLOCKCHAIN): DE LA MIȘCAREA CYPHERPUNK LA JP MORGAN CHASE	35
2.1 Fundamentele filozofice și ideologice ale Bitcoin.....	35
2.1.1 Ideologia libertariană și precursorii Bitcoin	35
2.2 Începuturile și dezvoltarea Bitcoin.....	38
2.2.1 Apariția Bitcoin	38
2.2.2 Atacuri și scandaluri legate de Bitcoin.....	40
2.2.3 Bula speculativă a criptomonedelor	41
3. CUM FUNCȚIONEAZĂ BITCOIN ȘI CUM POATE FI OPTIMIZAT	44
3.1 Funcțiile hash criptografice.....	44
3.2 O bază de date imutabilă (care nu poate fi modificată fără a se vedea acest lucru).....	48
3.2.1 Descompunerea unui bloc de date.....	48
3.2.2 Arborii Merkle	49
3.2.3 Nonce, sau manifestarea fizică a dovezii muncii	52
3.3 Semnături, ECDSA și adrese.....	56
3.4 Scriptul Bitcoin	64
4. BITCOIN ÎN VIAȚA REALĂ: PORTOFELE DIGITALE, ACTIVITATEA DE MINERIT ȘI ALTELE.....	74
4.1 Tipuri de utilizatori.....	74
4.2 Portofele digitale.....	75
4.3 Mecanisme de funcționare a portofelelor digitale.....	79
4.4 Activitatea de minerit	82
4.4.1 Bazinele miniere – mining pools	90
4.5 Evoluția Bitcoin	94
4.6 Utilizarea tehnologiei blockchain de către companii	96
4.6.1 Blockchain cu permisiune (permissioned blockchain) versus blockchain fără permisiune (permissionless blockchain).....	97
4.6.2 Potențiale utilizări ale tehnologiei blockchain	100
4.7 Situația criptomonedelor în România.....	109

5. STRATEGII DE ATAC ÎN REȚEAUA BITCOIN.....	114
5.1 Strategii de atac referitoare la bazine miniere.....	114
5.2 Atacul cu dublarea cheltuielilor	119
5.3 Atacuri prin cenzurarea tranzacțiilor	122
5.4 Mineritul egoist	124
5.5 Posibilități de apărare împotriva atacurilor	125
6. ETHEREUM ȘI CONTRACTELE SALE INTELIGENTE	139
6.1 Ethereum.....	143
6.2 Mașina Virtuală Ethereum (EVM).....	146
6.3 Exemple de utilizare a Ethereum.....	149
6.3.1 Utilizări de bază	149
6.3.2 Utilizări avansate.....	151
6.3.3 Utilizări amuzante.....	159
6.4 Situația actuală a tehnologiei blockchain și proiecte de viitor.....	160
6.5 Considerații finale despre tehnologia blockchain	180
7. CRIPTOMONEDELE ȘI LUMEA REALĂ – POT FI CRIPTOMONEDELE CONSIDERATE BANI?	184
7.1. Limbajul „criptic” al criptomonedelor	184
7.1.2 Monede „moderne”: monede electronice, monede digitale, monede virtuale și criptomonede	184
7.2. Conceptul de monedă – de la moneda marfă la inovațiile monetare și financiare moderne	194
7.2.1 Ce sunt banii? Evoluția conceptului de bani.....	194
7.2.2 Procesul de creare a banilor.....	200
7.2.3 Rolul băncii centrale și politica monetară.....	205
7.2.4 Alternative la banii emiși de statul național.....	212
7.2.5 Dimensiunea socială și politică a banilor.....	225
8. IMPLICAȚII DE SECURITATE ALE CRIPTOMOEDELOR.....	237
8.1 Utilizarea criptomonedelor pentru spălarea banilor și activități de crimă organizată.....	237
8.1.1 Criptomonede private și serviciile de mixer de criptomonede.....	238
8.1.2 Utilizarea criptomonedelor ca mijloc de spălare a banilor – cazul atacului malware Carbanak și Cobalt.....	247
8.2 Utilizarea criptomonedelor pentru alte activități ilegale	249
8.3 Corelarea utilizării criptomonedelor ca mijloace de plată alternative pentru evitarea impozitării.....	256
8.4 Utilizarea criptomonedelor pentru finanțarea terorismului.....	258
8.5 Criptomonedele ca armă utilizată la nivel de state	270
8.5.1 Finanțarea activităților de spionaj și război informațional prin utilizarea criptomonedelor	270
8.5.2 Utilizarea criptomonedelor pentru promovarea ideologiei extremiste.....	273
8.5.3 Utilizarea criptomonedelor pentru evitarea sancțiunilor economice.....	278

8.5.4 Utilizarea criptomonedelor pentru finanțarea sau manipularea alegerilor	285
8.6 Implicațiile extragerii criptomonedelor asupra securității energetice	291
8.7 Implicațiile criptomonedelor asupra stabilității financiare și a politicii monetare	295
8.7.1 Impactul asupra infrastructurii piețelor financiare	297
8.7.2 Impactul asupra altor intermediari și piețe financiare.....	298
8.7.3 Implicații asupra politicii monetare.....	298
8.7.4 Criptomonede emise de companii private – Studiu de caz Libra	302
8.8 Cum ar trebui să se implice autoritățile statului pentru a reduce riscurile aferente utilizării criptomonedelor?	321
 9. CONCLUZII	 326
 GLOSAR.....	 330
 BIBLIOGRAFIE.....	 340