

OBSAH

O AUTOROVI	V
ÚVOD	VII
1 ZÁKLADY TECHNOLOGIE KRYPTOMĚN	1
1.1 Definice kryptoměny	2
1.2 Historie bitcoinového systému	4
1.3 Vnitřní struktura bitcoinového systému	9
1.4 Struktura bitcoinové sítě	13
1.5 Struktura uživatelů bitcoinového systému	16
2 DOSAHOVÁNÍ KONSENZU	20
2.1 Důkaz prací	23
2.2 Důkaz prací s více hašovacími funkcemi	29
2.3 Důkaz podílem	32
2.4 Zastupitelský důkaz podílem	36
2.5 Důkaz důležitostí	40
2.6 Další typy důkazů	43
2.7 Vzájemné vztahy důkazů	47
2.8 Transakční poplatky	50
3 ANONYMITA	57
3.1 Ovlivnění míry anonymity při běžných transakcích	57
3.2 Dobrovolné snižování míry anonymity	59
3.3 Zvyšování míry anonymity	61
3.4 Kryptoměny se zvýšenou anonymitou	63
4 RIZIKOVÁ ANALÝZA	68
4.1 Uživatelé	69
4.2 Provozovatelé služeb	70
4.3 Software	72
4.4 Zneužití kryptoměn	76
4.5 Útoky na konsenzus	79
5 FUNKCIONALITA	82
5.1 Vznik kryptoměn	82
5.2 Zaujmout názvem	85
5.3 Komunitní využití	87
5.4 Kryptoměnové platformy	89
5.5 Návrh optimální kryptoměny	93

Obsah

6 EKONOMICKÁ VÝZNAMNOST	99
6.1 Získání a předzpracování dat	100
6.2 Duplicity v názvu a zároveň i v symbolu	102
6.3 Počet kryptoměn	104
6.4 Objem obchodů	106
6.5 Kryptoměnové indexy	108
ZÁVĚR	112
SUMMARY	119
SEZNAM ZDROJŮ	121
REJSTŘÍK	139