

Matematika bitcoinu | obsah

00 Proč? | Předmluva autora

01 Bitcoin je...

02 Bitcoin potřebuje počítač stroj

03 Bitcoin je počítačový program | Program je posloupnost instrukcí

04 Bitcoin je transakční P2P síť | Počítače v síti – Internet

05 Bitcoin je kódovaná komunikace | Číselné soustavy a kódování

06 Bitcoin je hra s velkými čísly | Velká čísla zahrávající si s „nekonečnem“

07 Asymetrická kryptografie | Diffie-Hellmanova výměna klíčů

08 Eliptické křivky jsou ladné | Operace modulo a cyklické grupy

09 ECC klíče | ECDSA | Secp256k1

10 Síla klíče | Jen zrníčko písku ve vesmíru

11 Jak důležitá je entropie | Shannonova entropie

12 Seed je váš klíč | Jak vzniká z náhodného čísla slovní seed

13 Meleme data na haši | SHA-256

14 Merkelovy stromy nám optimalizují strukturu

15 Bitcoinové adresy jsou dynamická čísla účtů

16 Bitcoinová transakce | Formát skriptu | Nejčastější opcodes

17 Těžba bitcoinů je hádání čísla za odměnu | Hledání nonce

18 Blockchain je nepřetržitelný řetěz | Koncepční diagram

19 Halving je chytré půlení odměny těžařům

20 Kvantové počítače | základy

21 Hrozba kvantových počítačů pro (b/B)itcoin?

Příloha A — Historia Magistra Vitae | Bitcoin prehistory

Příloha B — Shrnutí | Jak to teda celé funguje?

Příloha C — Genesis blok

Zdroje | Odkazy | Epilog

