

فهرست

فهرست	۵
پیش‌گفتار	۱۲
فصل نخست	۱۵
مفاهیم ابتدایی	۱۵
توضیحات برخی ابهامات حول محور بیتکوین	۱۵
چرا بیتکوین به وجود آمد و قرار است چه مشکلی را حل نماید؟	۱۵
معاملات کالا به کالا	۱۶
معایب معاملات کالا به کالا	۱۶
پول و چرایی پیدایش آن	۱۶
پول خوب چه مزیت‌هایی دارد؟	۱۷
نسبت عرضه به جریان	۱۹
ظهور بیتکوین	۲۰
آشنایی اولیه با مفاهیم پایه در تعریف بیتکوین	۲۲
سیستم متمرکز چیست و چه معایبی دارد؟	۲۲
بحران‌های بانکی	۲۲
تصاحب دارایی‌های مردم توسط دولت‌ها	۲۳
ابر تورم‌ها (Hyperinflation)	۲۳
مزیت‌های سیستم‌های غیرمتمرکز	۲۵
مقاوم در برابر دست درازی یا قفل کردن دارایی شما	۲۵
دسترسی جهانی	۲۵
امکان کنترل پول خود	۲۵
پوشش طیف گسترده‌تری از انسان‌ها	۲۶

- سیستم غیرمتمرکز قدرت گرفته از بلاکچین ۲۶
- مفهوم بلاک چین ۲۶
- سیستم همتا به همتا یا peer to peer ۲۸
- نقش نود های شبکه بیتکوین در بلاکچین ۲۹
- بیتکوین چیست؟ ۳۱
- نگاه کلی به نحوه کارکرد شبکه بیتکوین ۳۲
- امنیت شبکه بیتکوین ۳۳
- نگاهی به قیمت بیتکوین ۳۴
- مقایسه عملکرد قیمت بیتکوین در مقابل طلا ۳۴
- پرداخت ده هزار بیتکوین برای ۲ پیتزا ۳۸
- بیتکوینر ۳۹
- صل دوم: آشنایی با کیف پول های بیتکوینی ۴۱
- چرا به کیف پول نیاز داریم؟ ۴۱
- انواع کیف پول های بیتکوینی ۴۳
- نصب کیف پول الکتراام نسخه دسکتاپ ۴۳
- عبارات بازیابی یا mnemonic phrase ۴۵
- نحوه نگهداری عبارات بازیابی ۴۵
- بازیابی کیف پول از روی عبارات بازیابی ۴۸
- نصب کیف پول موبایلی Blue wallet ۴۹
- مشاهده آدرس بیتکوینی ۵۰
- فرمت آدرس های بیتکوینی ۵۱
- (Pay To Pubkey) P2PK ۵۲
- (Pay-to-Public-Key-Hash) P2PKH ۵۲

۵۲.....	(Pay-to-Script-Hash) P2SH
۵۲.....	(P2WPKH & P2WSH) Bech32
۵۲.....	(Pay-to-Taproot) P2TR
۵۲.....	فراوانی کاربرد آدرس های بیتکوینی
۵۲.....	ارسال بیتکوین های اولیه به شیوه P2PK و بررسی مشکلات آن
۵۴.....	کلیدهای خصوصی و عمومی
۵۵.....	تعریف entropy
۵۶.....	احتمال تولید کلمات بازیابی مشابه
۵۷.....	چه زمانی به کلید عمومی و چه زمانی به کلید خصوصی نیاز داریم؟
۵۷.....	کیف پول های سرد و گرم
۵۸.....	کیف پول های سخت افزاری
۵۸.....	نحوه راه اندازی کیف پول سخت افزاری بلاک استریم JADE
۶۴.....	کدام کیف پول را انتخاب نماییم؟
۶۵.....	حمله آچار فرانسه ۵ دلاری
۶۵.....	والتهای ناظر یا Watch-Only Wallet
۷۰.....	بیتکوین های تستی
۷۱.....	دریافت بیتکوین تستی
۷۲.....	ارسال بیتکوین تستی
۷۴.....	کیف پول های چند امضایی یا Multi Sign
۷۴.....	کاربرد کیف پول های چند امضایی
۷۴.....	راه اندازی کیف پول چند امضایی با کیف پول الکترا
۸۳.....	کیف پول های کاغذی
۸۵.....	کیف پول های Multi-Coin

- ۸۶..... ساختار HD Walletها
- ۸۷..... استانداردهای تولید عبارات بازیابی کیف پول
- ۸۷..... BIP39
- ۸۷..... Electrum v2
- ۸۷..... Aezeed
- ۸۸..... Muun
- ۸۸.....Slip39
- ۸۹..... نکاتی در مورد passphrase
- چرا برای نگهداری بیتکوین، بهتر است به جای کیف پولهای Multi coin از کیف پولهای "فقط بیتکوینی" استفاده کنیم؟
- ۸۹.....
- ۹۰..... افرادی که عبارات بازیابی خود را از دست داده‌اند
- فصل سوم: تراکنش‌های بیتکوینی، مفهوم UTXOها، مفهوم ماینینگ و بلاک‌ها در شبکه بیتکوین
- ۹۱.....
- ۹۲..... آشنایی با ممپول
- ۹۳..... آشنایی با مفهوم UTXO
- ۹۴..... مفهوم TXID یا Transaction ID در تراکنش‌های بیتکوینی
- ۹۵..... چه اطلاعاتی از TXID قابل استخراج است؟
- ۹۶..... بررسی تراکنش‌ها از طریق سایت mempool.space
- ۹۷..... محاسبه کارمزد پرداخت شده به ماینرها
- ۹۸..... چه تعداد تأیید در شبکه بیتکوین لازم است؟
- ۹۹..... چگونه از صحت تأیید بیتکوین ارسالی مطمئن شویم؟
- ۱۰۰..... Bump fee یا Replace-By-Fee (RBF) چیست؟
- ۱۰۲..... Child Pays for Parent چیست؟
- ۱۰۳..... نحوه رصد کردن منبع و مقصد تراکنش‌ها

۱۰۶.....	Dust attack مفهوم
۱۰۶.....	استفاده از مرورگر For
۱۰۷.....	بررسی تراکنش‌ها با وب سایت oxt.me
۱۰۹.....	فصل چهارم: نحوه ساخت بلاک و عملیاتی که ماینرها انجام می‌دهند
۱۱۰.....	وظیفه ماینرها در شبکه بیت کوین
۱۱۰.....	مفهوم اثبات کار
۱۱۱.....	مفهوم سختی شبکه
۱۱۲.....	فرمول تعیین سختی شبکه
۱۱۳.....	هش یا توابع هش (hash functions) چیست؟
۱۱۴.....	خصوصیت توابع هش
۱۱۵.....	انواع توابع هش
۱۱۵.....	بلاک هدر در بلاک‌های بیتکوینی
۱۱۶.....	نحوه ایجاد یک بلاک جدید
۱۲۱.....	انواع شیوه‌های ماینینگ
۱۲۱.....	۱: استفاده از استخرهای ماینینگ یا Mining pools
۱۲۲.....	مزایای استفاده از استخرهای ماینینگ
۱۲۲.....	معایب استفاده از استخرهای ماینینگ
۱۲۳.....	۲: Solo mining
۱۲۳.....	مزایای Solo mining
۱۲۳.....	معایب Solo mining
۱۲۴.....	ماینینگ خانگی بیتکوین
۱۲۴.....	برای پرداخت کارمزد کمتر به ماینرها، چه زمانی بیتکوین را جابه‌جا نمایم؟
۱۲۵.....	معرفی نرم افزار Mempool Bitcoin Fee Tracker

- نحوه محاسبه کارمزد تراکنش‌های بیتکوینی..... ۱۲۶
- مفهوم Virtual size..... ۱۲۷
- ۱- تعداد ورودی‌های تراکنش..... ۱۲۷
- ۲- تعداد خروجی‌های تراکنش..... ۱۲۸
- ۳- سختی اسکریپت‌ها (Script Complexity)..... ۱۲۸
- ۴- نوع تراکنش..... ۱۲۸
- ۵- چند امضایی بودن تراکنش..... ۱۲۸
- ۶- Witness Data (SegWit)..... ۱۲۹
- ۷- قابلیت Time-Locking..... ۱۲۹
- جلوگیری از Dust attacks..... ۱۲۹
- فصل پنجم: چگونه بیتکوین به دست بیاوریم؟..... ۱۳۱
- خرید بیتکوین بدون واسطه از افراد..... ۱۳۲
- نکاتی که در هنگام خرید بی واسطه از افراد می‌بایست رعایت نمود..... ۱۳۲
- معرفی نرم‌افزار Bisq..... ۱۳۲
- مفهوم Stable coins..... ۱۳۳
- Tether (USDT) و USD Coin (USDC)..... ۱۳۳
- مشکلات stable coin ها..... ۱۳۴
- خرید بیتکوین از صرافی‌های متمرکز یا CEX (Centralized Exchanges)..... ۱۳۴
- تنها دلیل استفاده از exchangeها..... ۱۳۵
- خالی فروشی چیست؟..... ۱۳۵
- داستان صرافی FTX..... ۱۳۶
- نمونه‌های خالی فروشی یا هک شدن صرافی‌های رمز ارز..... ۱۳۶
- خرید بیتکوین از صرافی متمرکز..... ۱۳۷

۱۳۷.....	مفهوم KYC
۱۳۸.....	نحوه خرید اسپات
۱۴۰.....	انتقال بیتکوین خریداری شده به کیف پول شخصی
۱۴۲.....	فروش بیتکوین در صرافی متمرکز
۱۴۴.....	انتخاب بستر انتقال دارایی ها در صرافی
۱۴۵.....	Swap یا تبدیل سایر رمز ارزها به بیتکوین
۱۴۷.....	حملات فیشینگ یا هک شدن والتها بر اثر اتصال به سایت‌های جانبی
۱۴۸.....	Swap کردن با مونرو
۱۴۸.....	کیف پول Cake Wallet
۱۴۹.....	تکنولوژی‌های استفاده شده در مونرو
۱۵۲.....	به دست آوردن بیتکوین از طریق ماینینگ
۱۵۲.....	نحوه محاسبه درآمد کسب شده از ماینینگ
۱۵۲.....	به دست آوردن بیتکوین از طریق ارائه خدمات یا فروش کالا
۱۵۴.....	آشنایی با سایت bitrefill
۱۵۵.....	بهترین روش خرید بیتکوین
۱۵۷.....	DCA یا Dollar-Cost Averaging چیست؟
۱۵۸.....	آشنایی با نرم‌افزار Buy bitcoin DCA manager
۱۶۱.....	فصل ششم: شبکه لایتینگ
۱۶۲.....	چرایی پیدایش شبکه لایتینگ
۱۶۲.....	مدت زمان تأیید تراکنش، طولانی است
۱۶۲.....	کارمزد در پرداخت‌های خرد و کوچک، گاهی مسأله‌ساز می‌گردد
۱۶۲.....	حفظ حریم خصوصی
۱۶۳.....	نصب و راه‌اندازی کیف پول Wallet of Satoshi

- ۱۶۲..... invoice دریافت بیتکوین بر بستر لایتینگ و آشنایی با مفهوم
- ۱۶۵..... on_chain تفاوت invoiceهای لایتینگ با آدرس‌های
- ۱۶۶..... لایتینگ پرداخت اینویس‌های لایتینگ
- ۱۶۶..... Lightning addresses چیست و چه کاربردی دارد؟
- ۱۶۷..... چگونه آدرس لایتینگ خود را به دست بیاوریم؟
- ۱۶۸..... تفاوت لایتینگ آدرس‌ها با invoiceهای لایتینگ
- ۱۶۸..... شارژ کیف پول‌های لایتینگ
- ۱۶۹..... روش استفاده شده در شبکه لایتینگ
- ۱۷۰..... مفهوم Capacity و Inbound و Outbound در شبکه لایتینگ
- ۱۷۵..... نصب و راداندازی کیف پول لایتینگ الکترام
- ۱۸۲..... Submarin Swap
- ۱۸۴..... پشتیبان‌گیری از کانال
- ۱۸۵..... پشتیبانی از آدرس‌های لایتینگ در والت الکترام
- ۱۸۶..... بستن کانال
- ۱۸۶..... انواع شیوه‌های بستن کانال
- ۱۹۰..... نصب و راداندازی کیف پول لایتینگ Phoenix
- ۱۹۳..... خرید ظرفیت و اریز
- ۱۹۷..... نکاتی در مورد استفاده از کیف پول‌های لایتینگ
- ۱۹۸..... خرید و به دست آوردن بیتکوین لایتینگ
- ۲۰۳..... پیوست؛ واژه‌نامه