ثروت سازی در بیت کوین، بلاکچین و ارزهای دیجیتال

مدرسه موفقیت

مهندس محمد طیب طاهر

محمد طیب طاهر

مدرس دوره



رتبه ۳۰۰ کنکور سراسری ریاضی
مهندسی برق-کنترل (دانشگاه علم و صنعت – رتبه ۱)
مشاور وزیر ارتباطات و فناوری اطلاعات (۱۳۹۸-۱۳۹۵)
مشاور ستاد مبارزه با قاچاق کالا و ارز (۱۳۹۷ تا اکنون)
هم بنیان گذار صرافی دریابیت
هم بنیان گذار مجموعه سرمایه گذاری تیک وست
موسس کوچینگ کسب و کار تارا
فعال حوزه بلاکچین
عضو سازمان نصر
عضو انجمن ملی بلاکچین

تکامل پول



کریپتو کارنسی | پول دیجیتالی | کارت های پلاستیکی | پول کاغذی | سکه فلزی | طلا | مبادله کالا به کالا

اعتبار در ایران



اولین بانک تاریخ ایران / ۱۲۶۷ ه.ش

به دستور ملکه انگلیس برای پرداخت وام به ناصرالدین شاه

وام برای دولت / سران

Finnohack

Bitcoin,
The 2008 Mysterious Birth

در ۳ ماه آگوست تا اکتبر ۲۰۰۸ میلادی؛

- در میانه بحران اقتصادی ایالات متحده، دامنه Bitcoin.org به ثبت رسید (۱۸ آگوست)

- از ۱۲ تا ۱۶ سپتامبر، آرماگدون اقتصادی رخ داد؛
  - دومینوی ورشکستگی به بانک های بزرگ رسید (Lehman and Merrill) (جمعه)
  - بانک امریکا (Bank of America) موسسه مالی Merrill را به قیمت ۵۰ میلیارد دلار خرید! (شنبه)
  - دولت ایالات متحده و انگلستان از Barclays برای خرید Lehman حمایت نکردند. (یکشنبه)
  - موسسه مالی Leman Brothers بزرگترین ورشکستگی تاریخ ایالات متحده را رقم زد. (دوشنبه)
  - برای متوقف کردن دومینو، دولت ایالات متحده، بودجه ۷۰۰ میلیارد دلاری اختصاص داد! (سه شنبه)



An Alternative Financial System

- Cost of Financial Crisis for U.S. Government: $2.5 trillion
- Any better time for the birth for one (or The) Alternative?

Bitcoin, A New Generation of Money!

- هزینه بحران اقتصادی برای دولت ایالات متحده، حدود ۲.۵ تریلیون دلار برآورد شده است
- اکنون زمان مناسب برای تولد جایگزین (یا تنها جایگزین) است؟

بیت کوین، نسل جدید پول!

Satoshi Nakamoto
(Oct 2008)



> It's completely decentralized, with no central server or trusted parties, because everything is based on *crypto proof* instead of *trust* … "

SuperSmart Innovation:
Is it really a “New Generation of Money”?

- Gold-Based Money
- Fiat Money



What is Money by the way?

Fungibility = معاوضه پذیری
Scarcity = محدودیت وجودی
Divisibility = قابلیت تفکیک
Durability = ماندگاری در طول زمان
Transferability = قابلیت انتقال
Liquidity = تسویه پذیری
Legitimacy = مشروعیت

Bitcoin Design
Managerial Big Picture, and the Idea

One Key point in Bitcoin is that there is No Central Entity to IDENTIFY people.

Bitcoin, is giving us a new Definition for Identity and Ownership.

To catch up the Architecture of Bitcoin, one should deeply understand the following concepts;

...



Bitcoin General Overview

Identity and Ownership in Bitcoin, is JUST a string of bits!



This is the method:

For Coins, there is a Private Key, a 256 - bit “randomly generated” number.

Question: Who is the Owner of this Coin?

Answer: Whoever Knows this Private Key! Easy!

Bitcoin, Identity and Transaction

There is a known function, we call it F(), which is extremely complicated.

If you apply this function on Private Key, what you get is “Public Key”.

Public Key = F (Private Key).

To be Clear:

Public Key is pretty much similar to the ATM Card Number (or Email Address).

And Private Key is the PIN Number (or Password).

- Everyone may know Public Key. It is Public!
- The only one who has access to the Coin, is the one who knows the Private Key.
- Your Public Key is used for other people to make a payment to you.

Public Key and Public Key

A Sample of Private Key;

571ae3370f84d2c6c4f6cb857146f32bcdb3bdaf14d105f30b5dd93efde17a44

And a Sample of Public Key;

1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

This is in fact Satoshi's Public Key in Genesis Block! There is 50BTC in it since Jan 2009. Who knows the related Private Key (F inverse of this number)?

Genesis Block:
https://www.blockchain.com/btc/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

کیف پول ارز دیجیتال

یک کیف پول ارز دیجیتال، نرم‌افزار یا سخت‌افزاری است که ارزهای دیجیتال را ذخیره، دریافت و ارسال می‌کند.



یک کیف پول ارز دیجیتال، نرم‌افزار یا سخت‌افزاری است که ارزهای دیجیتال را ذخیره، دریافت و ارسال می‌کند.

برای کار با کیف پول ارز دیجیتال نیاز نیست بدانید چگونه کار می‌کند، همان طور که برای کار با اینترنت نیاز نیست با زیرساخت‌های شبکه جهانی وب آشنا باشید. امروزه بیشتر کیف پول‌ها طراحی بسیار ساده و کاربرپسندی دارند و ارسال و دریافت ارز دیجیتال در آنها به‌سادگی ارسال و دریافت یک پیامک است.

عبارت بازیابی (بک‌آپ) کیف پول چند کلمه انگلیسی (معمولاً ۱۲ یا ۲۴ کلمه) است که از کلید خصوصی تولید شده است. مانند کلید خصوصی، نباید این عبارت را هم به کسی بدهید. اگر کیف پول شما پاک شود، با داشتن این کلمات می‌توانید دارایی خود را دوباره بازیابی کنید.

یادتان باشد بیشتر کیف پول‌ها به‌جای خودِ کلید خصوصی، به شما کلمات بازیابی ارائه می‌دهند که از نظر فنی همان کلید خصوصی ندارد و با آن فرقی ندارد.

انواع کیف پول ارز دیجیتال

کیف پول موبایل



به‌صورت یک برنامه روی تلفن همراه شما نصب می‌شوند.

کیف پول تحت‌وب



روی یک سایت پیاده شده است و می‌توانید با مرورگرهای اینترنت (مثل گوگل کروم، فایرفاکس و ...) به آن دسترسی پیدا کنید.

افزونه مرورگر



روی مرورگرهایی مانند گوگل کروم نصب می‌شوند و تراکنش‌ها از طریق مرورگر انجام می‌شود.

کیف پول دسکتاپ



نرم‌افزاری است که روی کامپیوترهای شخصی و سیستم‌عامل‌های ویندوز، لینوکس و مک نصب می‌شود.

کیف پول سخت‌افزاری

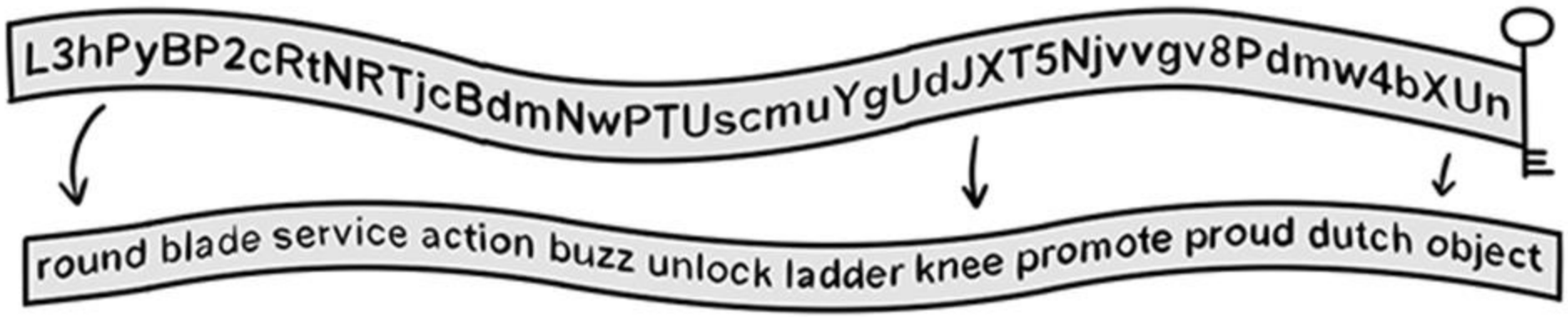


دستگاه‌های فیزیکی برای ذخیره سازی امن‌تر ارزهای دیجیتال.
برای سرمایه‌های سنگین مناسب هستند.

کیف پول کاغذی



همان کلید خصوصی یا عبارات بازیابی کیف پول است که روی کاغذ چاپ شده است.


L3hPyBP2cRtNRTjcBdmNwPTUscmuYgUdJXT5Njvvgv8Pdmw4bXUn
round blade service action buzz unlock ladder knee promote proud dutch object

01

کیف پول‌های موبایل به صورت یک برنامه روی تلفن همراه نصب می‌شوند. ازآنجاکه امروزه تقریباً هر فرد در هر کجا که باشد یک گوشی هوشمند در جیبش دارد، کیف پول‌های موبایلی را می‌توانیم پرکاربردترین نوع کیف پول بدانیم.



کیف پول تراست (Trust Wallet)

02

کیف پول‌های مبتنی بر وب (Web Wallet) ساده‌ترین کیف پول از نظر دسترسی و راحتی کار هستند. برای استفاده از این کیف پول‌ها فقط کافی است در هر دستگاهی از مرورگر اینترنتی استفاده شود. با این حال، ازآنجاکه این کیف پول‌ها کلید خصوصی را روی سرورهای اینترنتی ذخیره می‌کنند، ریسک هک‌شدن یا مسدودشدن بیشتری دارند.



کیف پول بلاک چین (Blockchain.com)

03

یکی دیگر از کیف پول‌های پرطرفدار سال‌های اخیر، کیف پول‌هایی هستند که در قالب افزونه‌های (Extension) مرورگر کار می‌کنند. مزیت اصلی این کیف پول‌ها این است که می‌توانند مرورگرهای معمولی شما را به مرورگر بلاک چین تبدیل کنند. با استفاده از این افزونه‌ها می‌توانید وارد پلتفرم‌های غیرمتمرکز مختلف شوید و با آنها تعامل داشته باشید.



کیف پول متامسک (Metamask)

04

کیف پول دسکتاپ، نرم‌افزاری است که روی کامپیوترهای شخصی و سیستم‌عامل‌های ویندوز، لینوکس و مک نصب می‌شود. این کیف پول‌ها مانند کیف پول موبایل کلیدهای خصوصی را روی خودِ دستگاه ذخیره می‌کنند.

کیف پول اکسودوس (Exodus)

05

کیف پول‌های سخت‌افزاری (Hardware Wallet) **سردترین** گاوصندوق‌های فیزیکی برای نگهداری دارایی‌های دیجیتال هستند. این کیف پول‌های غیرامانی، دستگاه‌هایی هستند که به‌طور ویژه برای نگهداری آفلاین و ایمن ارزهای دیجیتال طراحی می‌شوند.

در حقیقت کیف پول‌های سخت‌افزاری با پروتکل‌های امنیتی‌ای که دارند اجازه نمی‌دهند کلید خصوصی بدون اجازه خارج شود و این یعنی خیال راحت است که هیچ‌کس جز صاحب کیف پول به کلیدهای خصوصی دسترسی ندارد.



کیف پول سخت‌افزاری

06

کیف پول کاغذی همان کلید خصوصی یا عبارات بازیابی کیف پول است که روی کاغذ چاپ شده است.



به‌دلیل خطراتی که این روش دارد، ذخیره ارز دیجیتال در کیف پول کاغذی تقریباً منسوخ شده است و کاربرد کمتری نسبت به سایر روش‌های ذخیره‌سازی دارایی‌های دیجیتال دارد.

با این حال، اگر باز هم این روش را برای ذخیره دارایی‌ها ترجیح داده می شود، می‌توان به وب‌سایت‌های ویژه ایجاد کیف پول کاغذی مثل BitAddress مخصوص کیف پول کاغذی بیت کوین مراجعه کرد.

بهترین کیف پول‌های ارز دیجیتال در سال ۲۰۲۱

