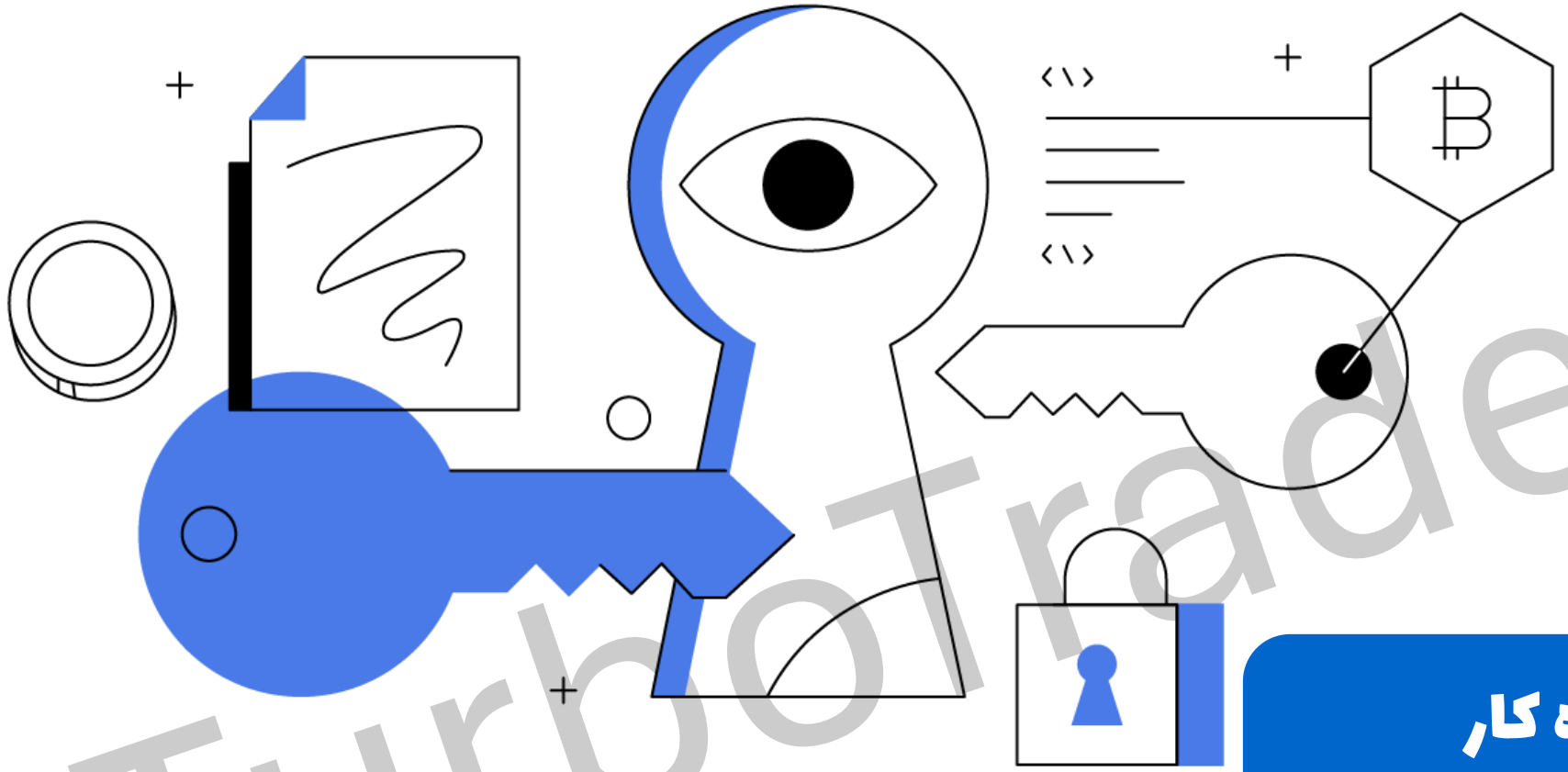
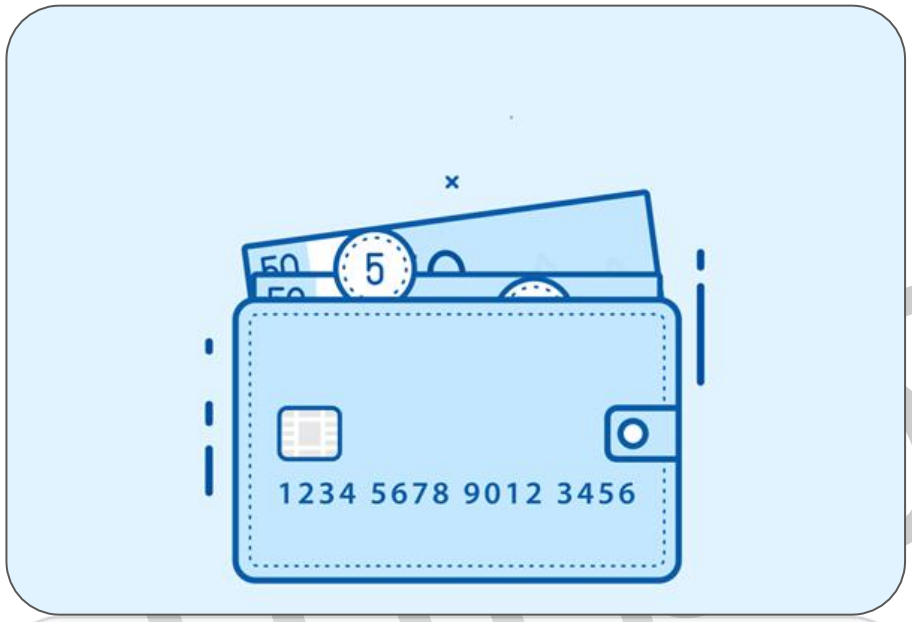


نگاهی به نحوه کار
کلید خصوصی و کلید عمومی

Introduction to Public Key and
Private Key Cryptography

مدرس : مهندس فرشید میرزائی

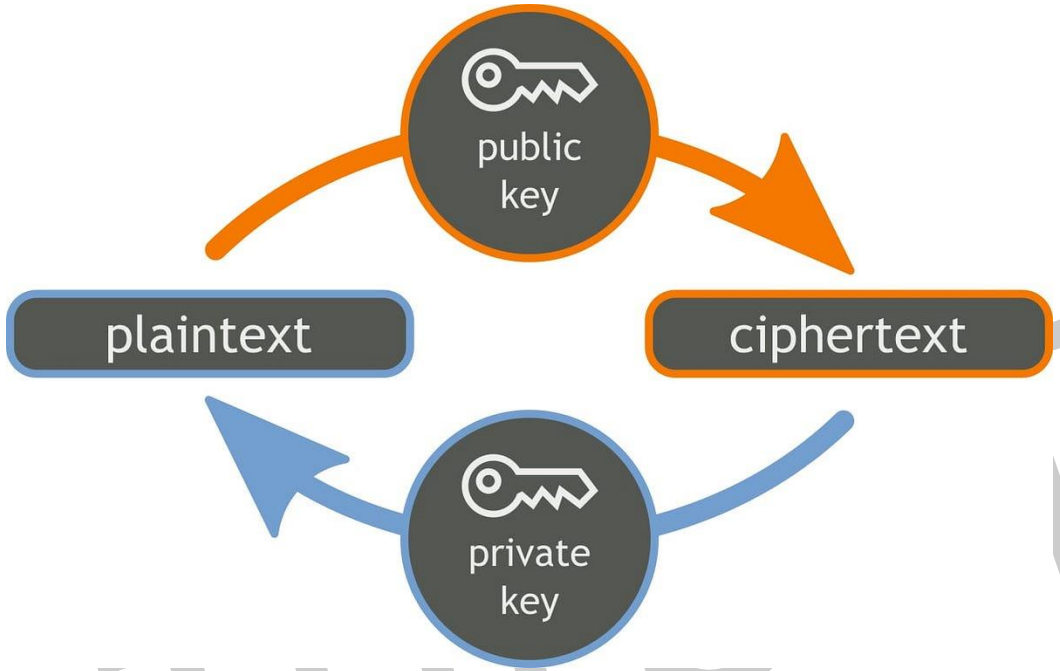
کیف پول ارزهای دیجیتال – وظیفه کیف پول



- همونطور که همه میدونیم ، کیف پول ها وظیفه نگهداری و انتقال دارایی های مارو بر عهده دارند . بطور کلی کیف پول ها واسط بین ما و شبکه بلاکچین هستند .

- در واقع کیف پول ها درخواست های مارو برای تایید شدن به بلاکچین ارسال میکنند تا بعد از اعتبار سنجی توسط نود ها ، درخواست انجام بشه .

کیف پول ارزهای دیجیتال – کلید عمومی و خصوصی

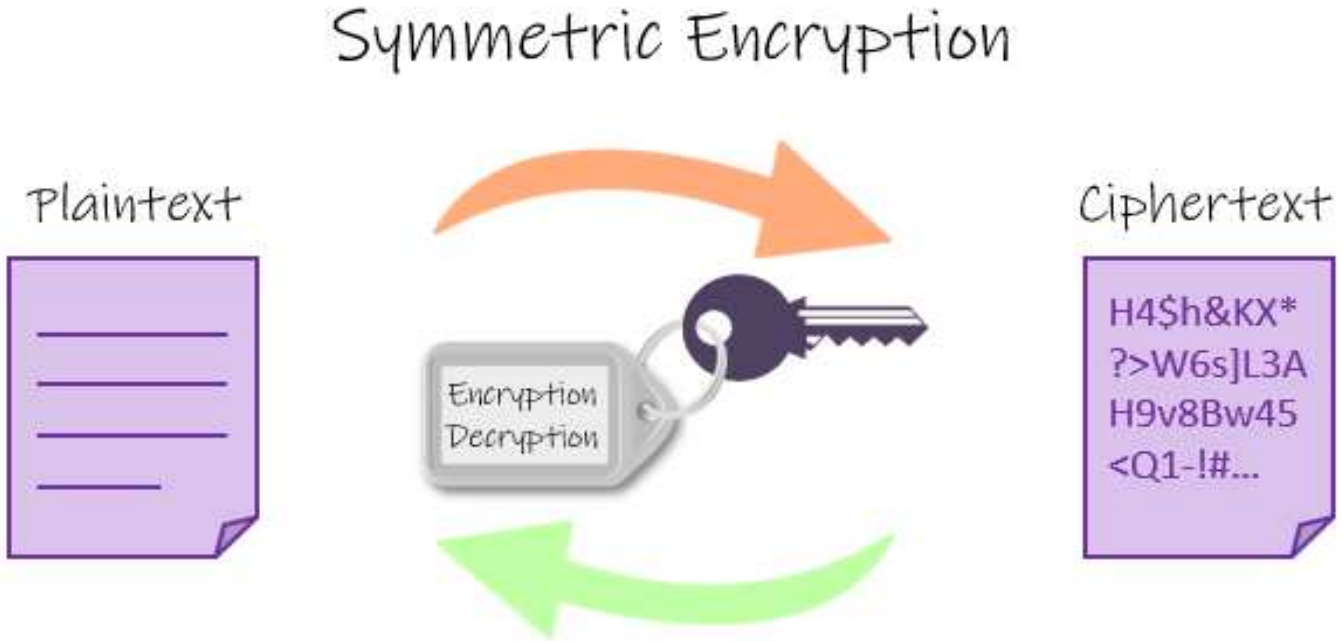


- تمام این فرایند انتقال با استفاده از کلید عمومی و کلید خصوصی انجام میگیره ، همونطور که گفتیم کلید عمومی مشابه شماره کارت شما برای دریافت ارزدیجیتال و کلید خصوصی هم مثل رمز عبور کارت شما برای دسترسی به کیف پولتون هست .
- اما اینها صرفا یک توضیح کلی بود و بهتره دقیق تر این مفاهیم رو بررسی کنیم .

کیف پول ارزهای دیجیتال – نحوه ساخت

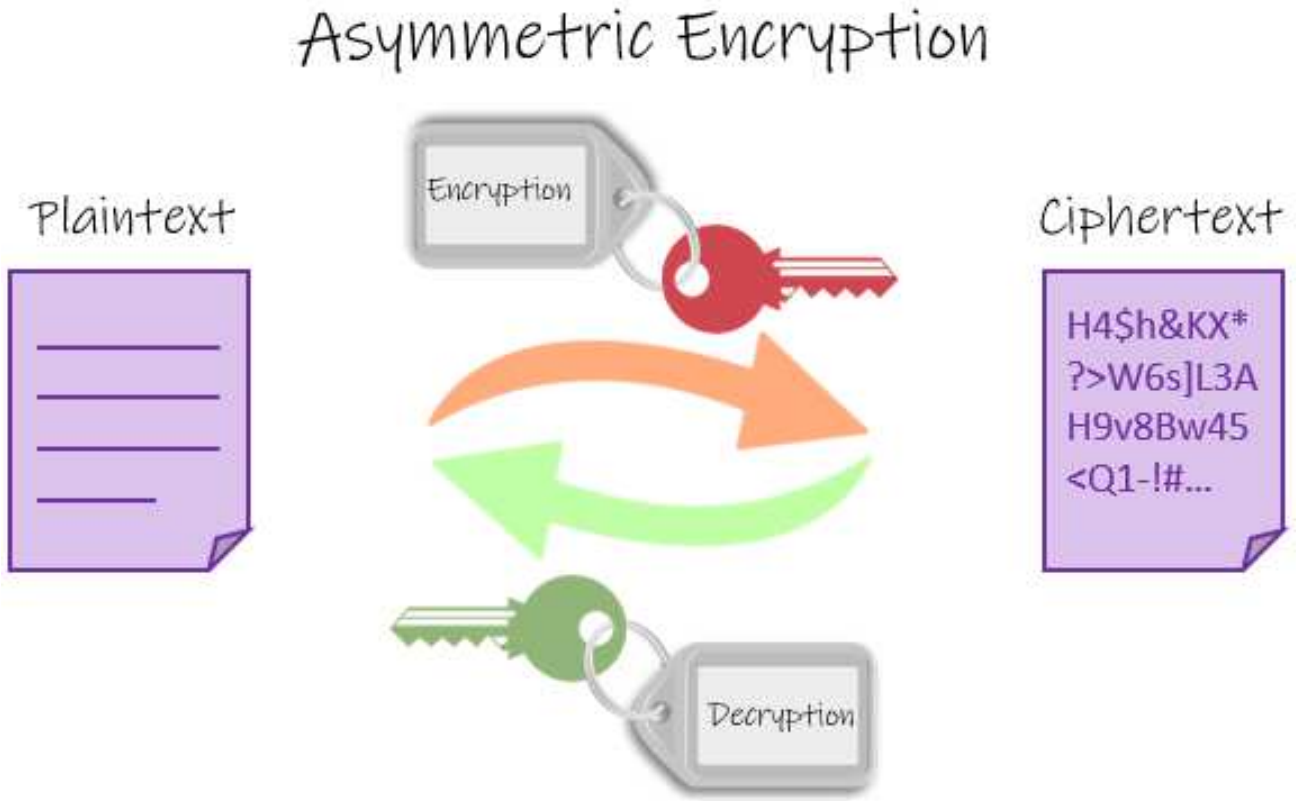
- وقتی صحبت از کلید عمومی و خصوصی میشه ، حتما ما به دنبال امنیت هستیم یا به عبارتی رمزنگاری و رمزگشایی !
- به همین دلیل بهتره به سراغ الگوریتم های رمزنگاری بریم ، برای رمز کردن پیامی که قصد ارسال اون رو داریم .
- در حوزه کریپتو کارنسی به دو دلیل نیاز داریم که از کریپتوگرافی استفاده کنیم :
  1. امنیت دارایی های خودمون
  2. امنیت انتقال دارایی ها (تشخیص و تایید درست انتقال دارایی از فرستنده X به گیرنده Y توسط ولیدیتور ها)

الگوریتم های رمزنگاری - رمزنگاری متقارن



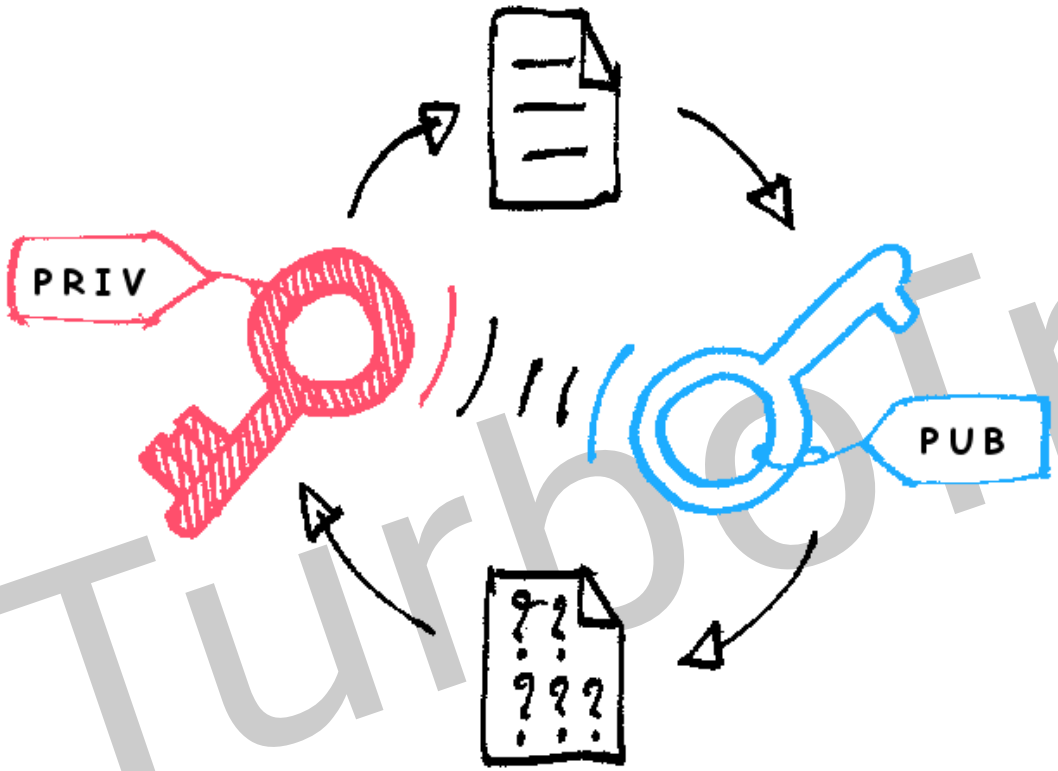
- در رمزنگاری متقارن که یک الگوریتم قدیمی هست ، از یک کلید مشترک به جهت رمزنگاری و رمزگشایی استفاده میشه .
- در این سیستم فرستنده و گیرنده باید این کلید مشترک رو در اختیار داشته باشند تا بتونن پیام های هم رو رمزگشایی کنند .
- مشکل بزرگ این الگوریتم ، به سرقت رفتن کلید در مسیر انتقال اون از یک سمت به سمت دیگر بود .

الگوریتم های رمزنگاری - رمزنگاری نامتقارن



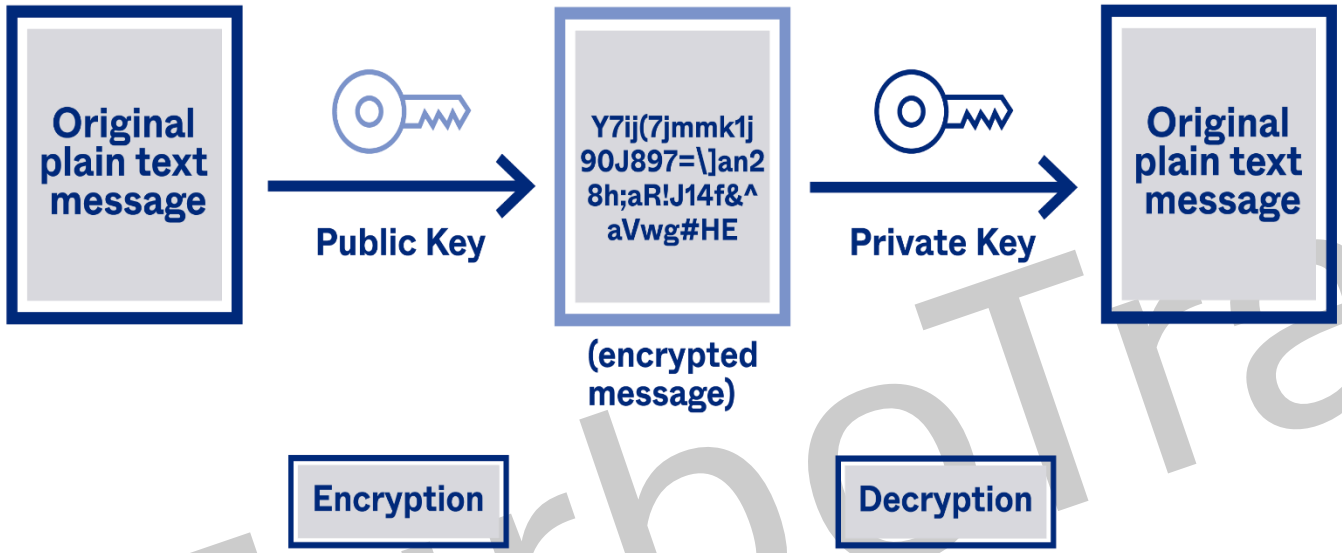
- بر خلاف رمزنگاری متقارن که فرستنده و گیرنده از یه کلید برای رمزنگاری استفاده میکردن؛ در رمز نگاری نامتقارن از یک جفت کلید (عمومی و خصوصی) که با محاسبات ریاضی به هم وصل شدن، استفاده میکنند.

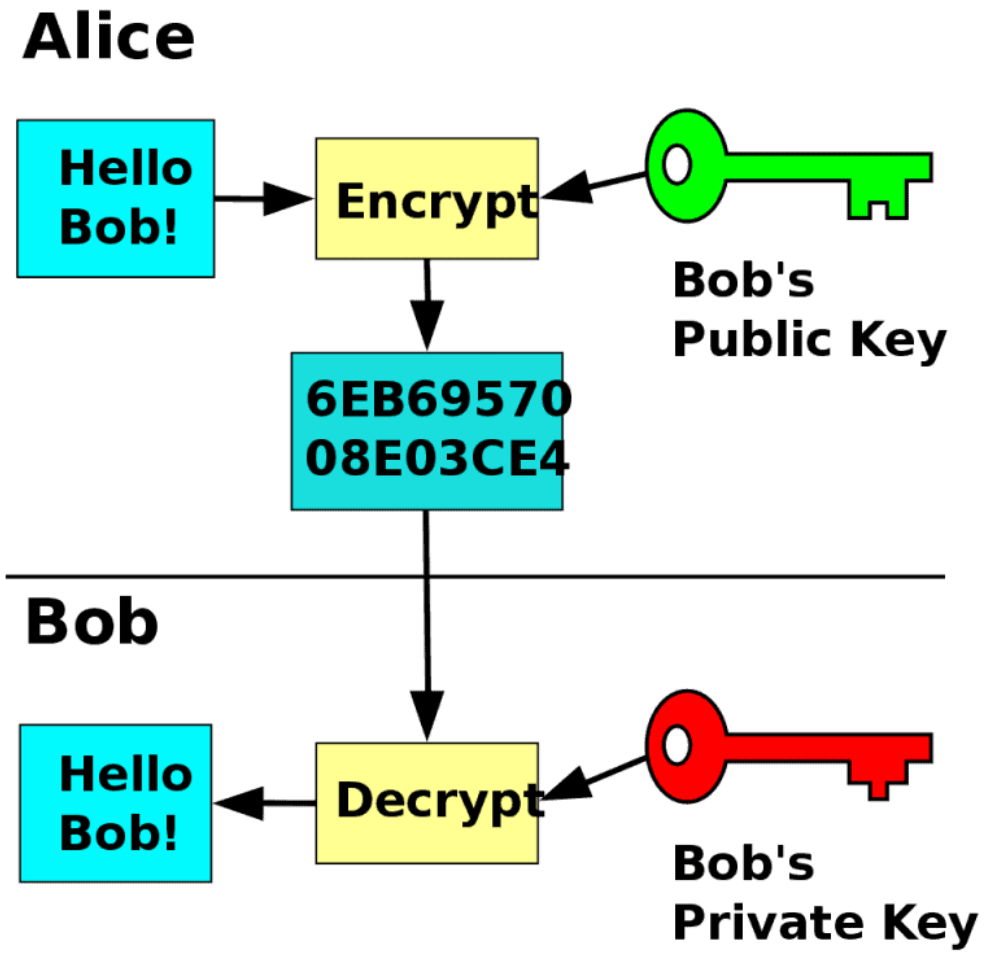
الگوریتم های رمزنگاری - رمزنگاری نامتقارن



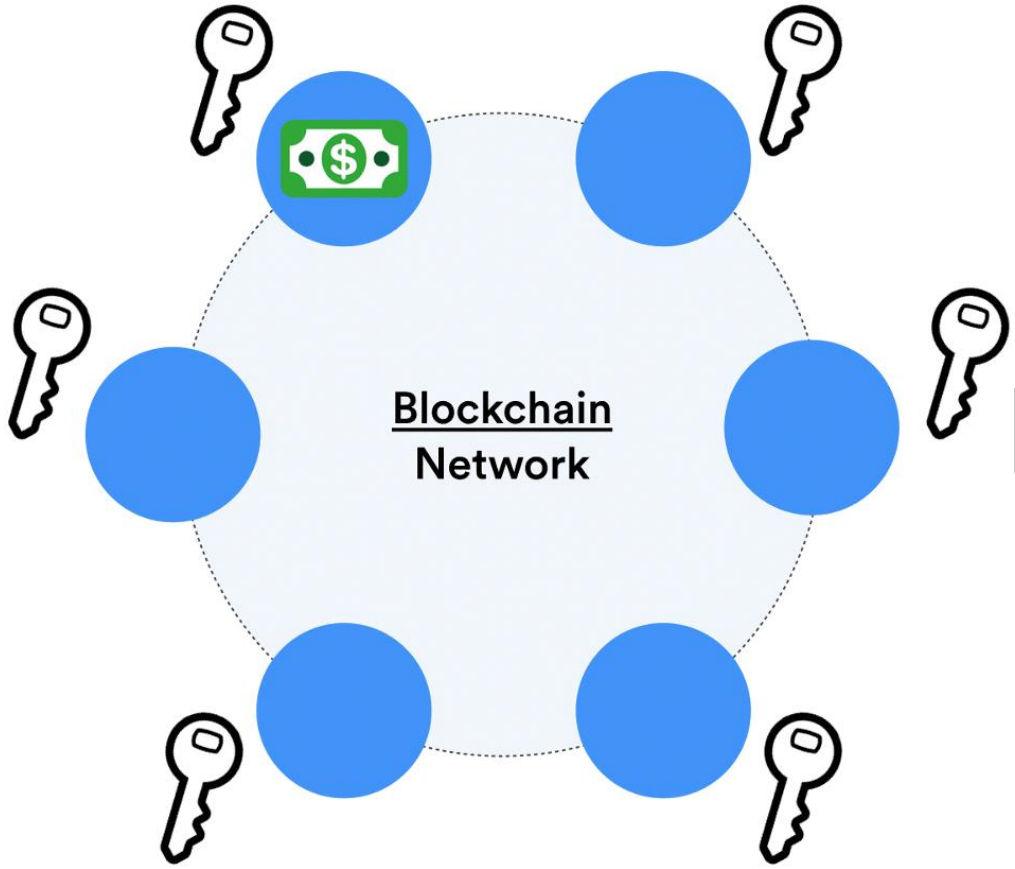
در این سیستم کلید های خصوصی هر کسی در اختیار خودش هست و ما برای ارسال پیام محرمانه به اون شخص (مثلا شخص X) ، با استفاده از کلید عمومی خودش ، اون رو رمزنگاری میکنیم و تنها کسی که میتونه اون رو رمزگشایی کنه ، فقط خود شخص (X) هست چون دارنده کلید خصوصی هست .

الگوریتم های رمزنگاری - رمزنگاری نامتقارن - مثال





❖ چرا با استفاده از کلید عمومی عملیات رمزنگاری رو انجام میدیم ؟



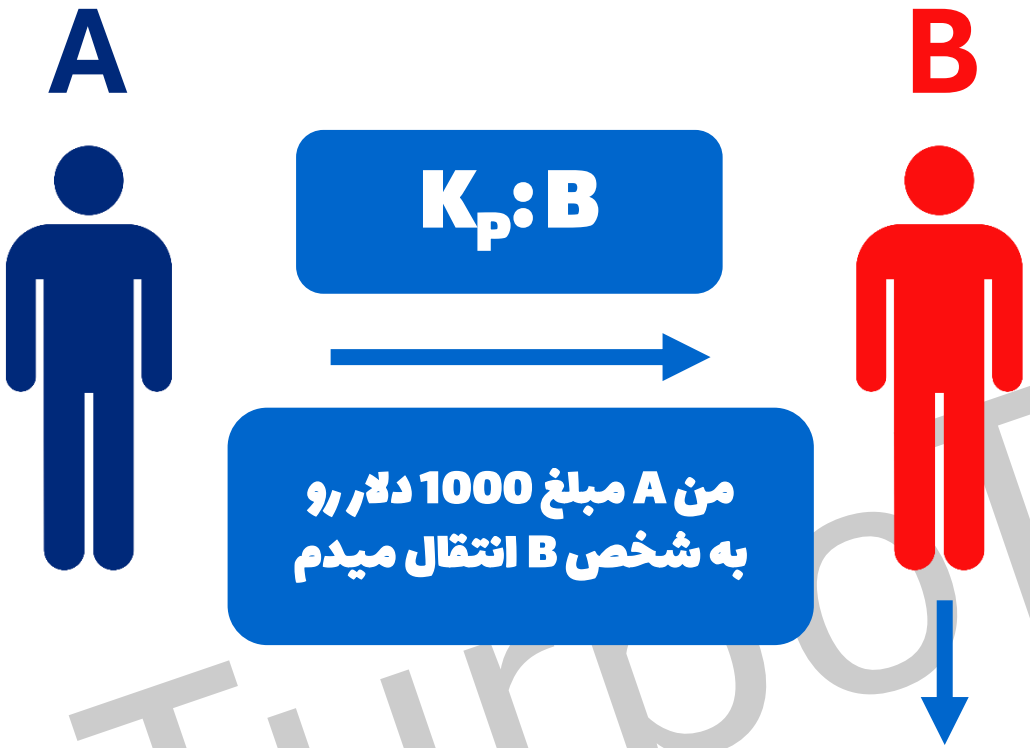
سناریوی انتقال دارایی با استفاده از کلید خصوصی و کلید عمومی

مدرس : مهندس فرشید میرزائی

سناریو انتقال دارایی - 1

- در این سناریو دو شخص A و B حضور دارند که فرد A قصد انتقال ۱۰۰۰ دلار به شخص B رو داره .

- برای اینکه A دارایی رو به B انتقال بده یک پیام ایجاد میکنه و اون رو با استفاده از کلید عمومی B (K_P) رمزگذاری میکنه و به B ارسال میکنه .



- B که پیام رو دریافت کردبا استفاده از K_S پیام رو باز میکنه و میگه بله درسته سکه ها به من منتقل شد ، ممنون .

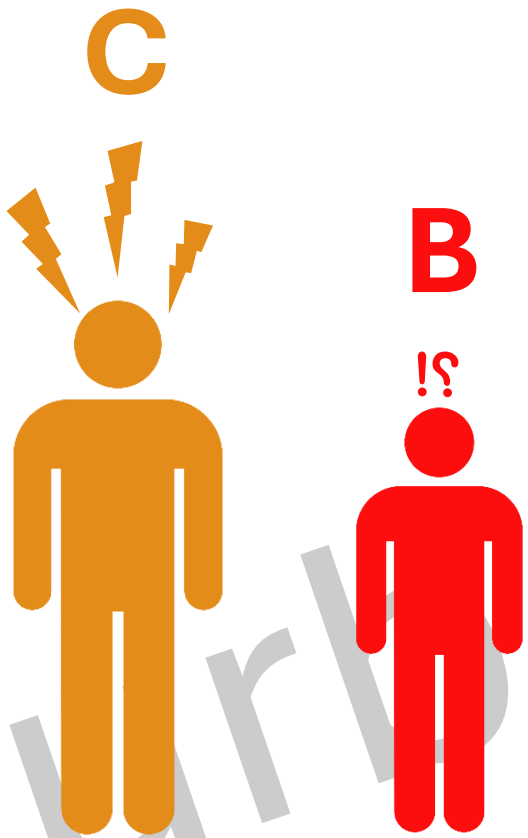
مدرس : مهندس فرشید میرزائی

سناریو انتقال دارایی - 2

- حالا فرض کنید B برای خرید یک محصول سراغ فرد C میره و میخواد اون ۱۰۰۰ دلار رو به شخص C منتقل کنه .

- پس مجدد یک پیام ایجاد میکنه برای شخص C و با استفاده از کلید عمومی شخص C اون رو رمزگذاری میکنه و برای فرد C ارسال میکنه .

سناریو انتقال دارایی - 3



- اینجا C به B شک میکنه و میگه از کجا معلوم این پولی که داری بهم میدی معتبر و مال خودت باشه ؟ شاید پول کس دیگه ای هست !؟
- بنظر شما چه راهکاری وجود داره که B بتونه اثبات کنه پول مال خودش هست ؟!
- اینجاست که امضای دیجیتال به کمکمون میاد .

Digital Signature in Blockchain

امضای دیجیتال در بلاکچین

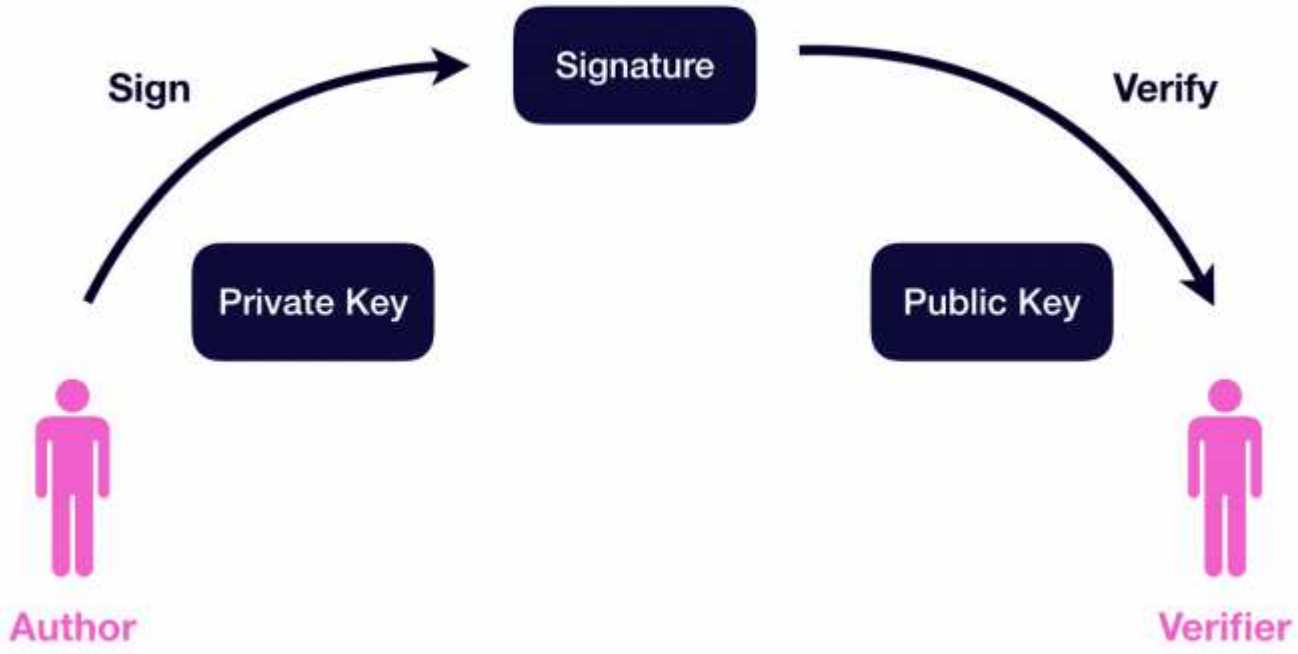
مدرس : مهندس فرشید میرزائی

امضای دیجیتال (Digital Signature) چیست؟

- امضای دیجیتالی مکانیسم رمزنگاری است که برای تأیید صحت و یکپارچگی داده های دیجیتال استفاده میشه . امضای دیجیتال رو میتونیم نسخه ی دیجیتالی امضاهای دستی در نظر بگیریم که در دنیای کامپیوتر ها امنیت و پیچیدگی خیلی بالاتری داره .

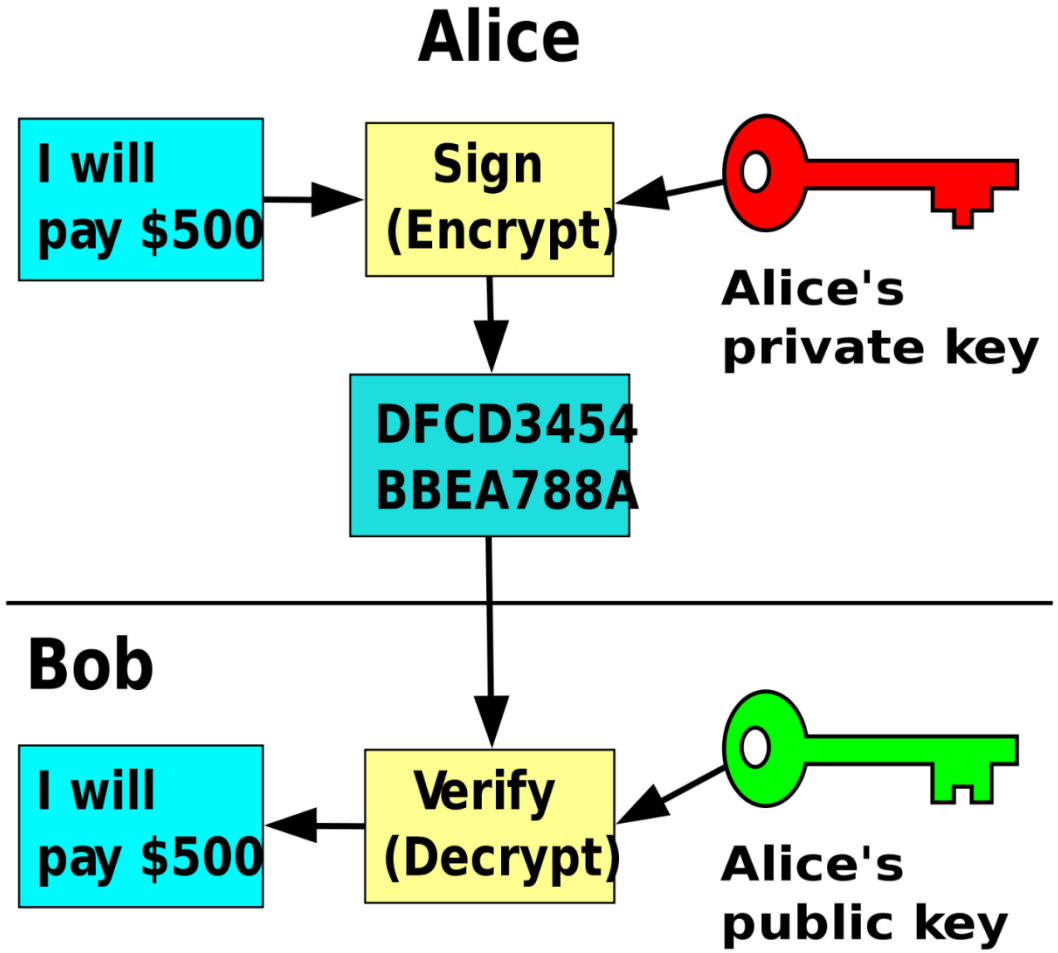
- امضای دیجیتال رو اینطوری درنظر بگیرید که برای عدم تغییر یک پیام بصورت کد ، در طول مسیر به اون متصل میشه .

امضاهای دیجیتالی چگونه کار می کنند؟



فرایند امضای دیجیتال توسط کلید خصوصی فرستنده انجام میگیره ، یعنی فرستده با استفاده از کلید خصوصی خودش پیام رو امضا میکنه و ارسال میکنه ، گیرنده میتونه با استفاده از کلید عمومی فرستنده تشخیص بده که آیا این پیام از طرف فرستنده واقعی (صاحب همون کلید خصوصی) ارسال شده یا نه .

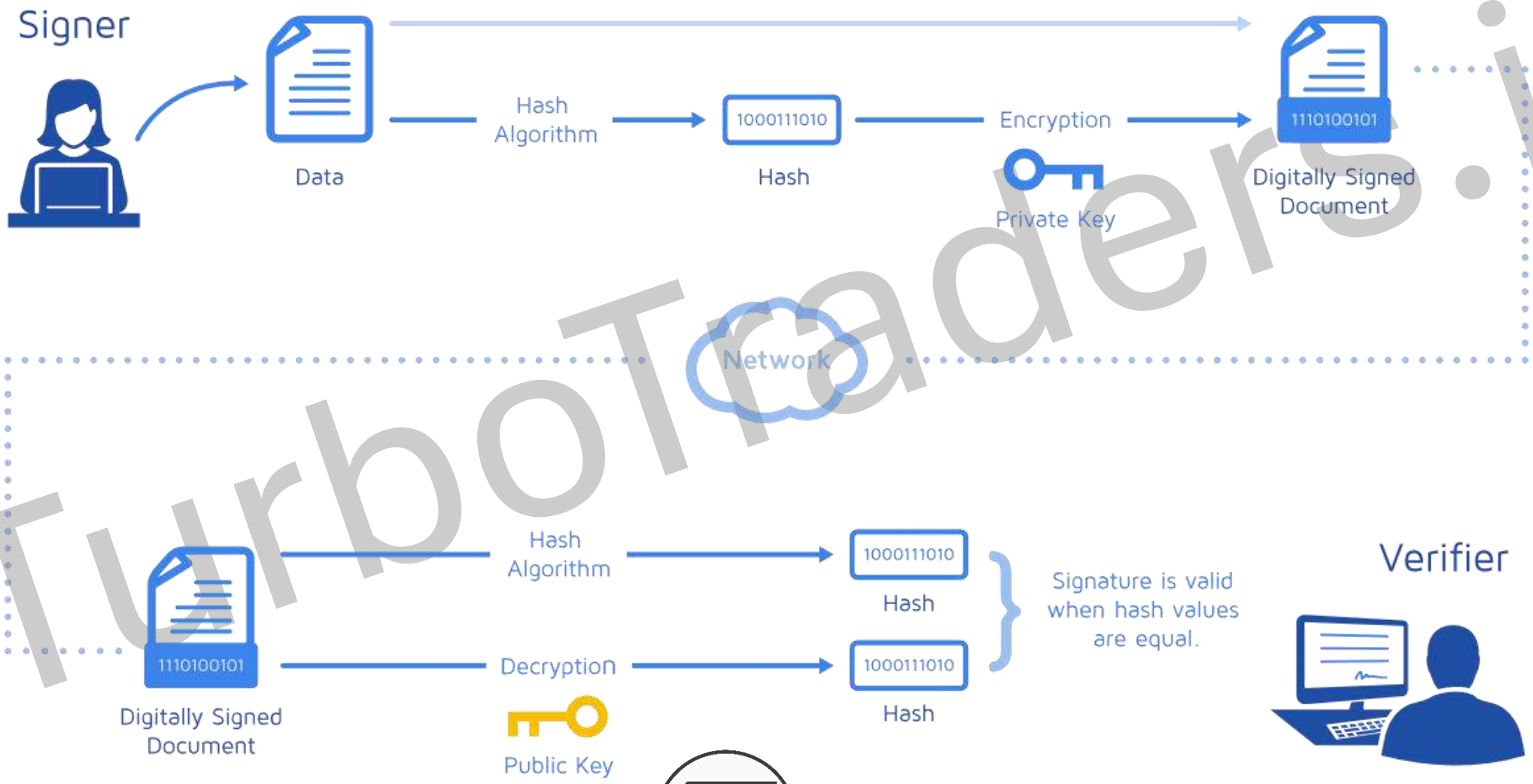
شبکه تراکنش ها در بلاک چین چگونه کار می کند؟



- آلیس قصد ارسال ۵۰۰ دلار به باب رو داره ، پس اون رو با کلید خصوصی خودش امضا میکنه و ارسال میکنه ، باب اون رو دریافت میکنه و با استفاده از کلید عمومی آلیس میتونه اون پیام رو مشاهده کنه !
- نکته ی مهم در اینجا اینه که باب برای مشاهده و اعتبارسنجی پیام نیازی به کلید خصوصی آلیس نداره و کلید خصوصی برای اعتبار سنجی هویت آلیس پیش خودش باقی میمونه .

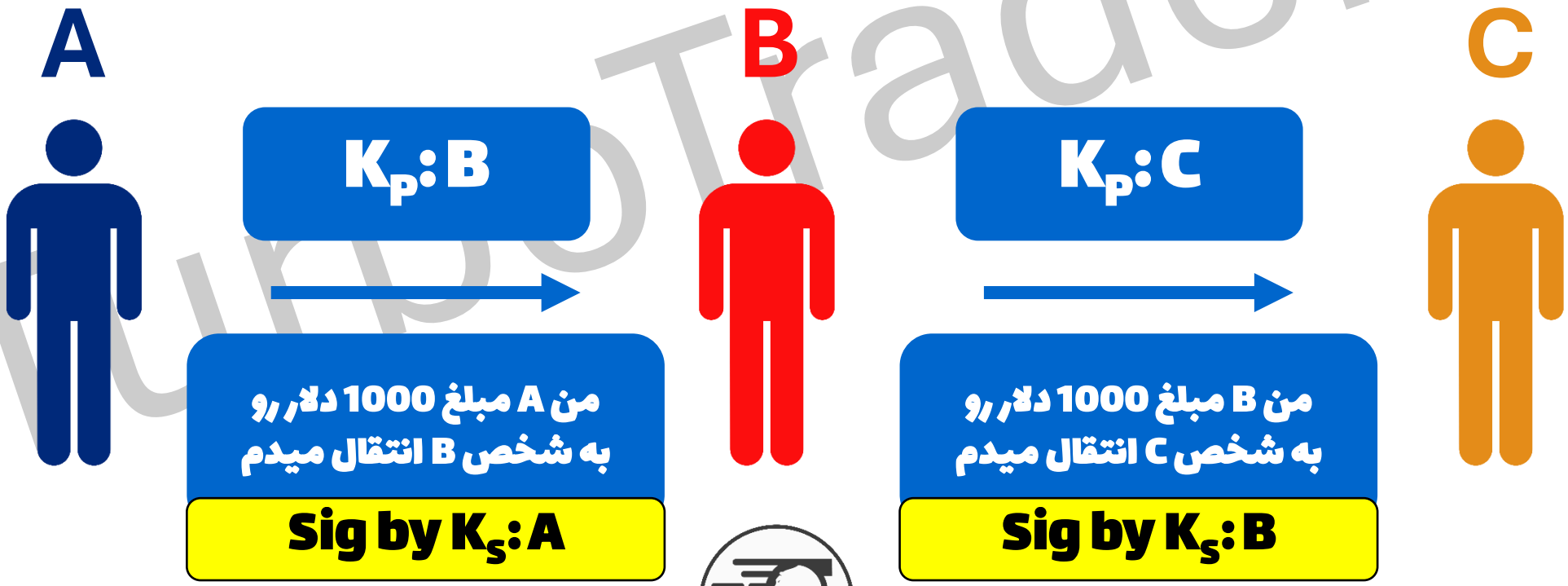
مدرس : مهندس فرشید میرزائی

مثال جمع بندی امضای دیجیتال – ارسال تراکنش ها برای نود ها

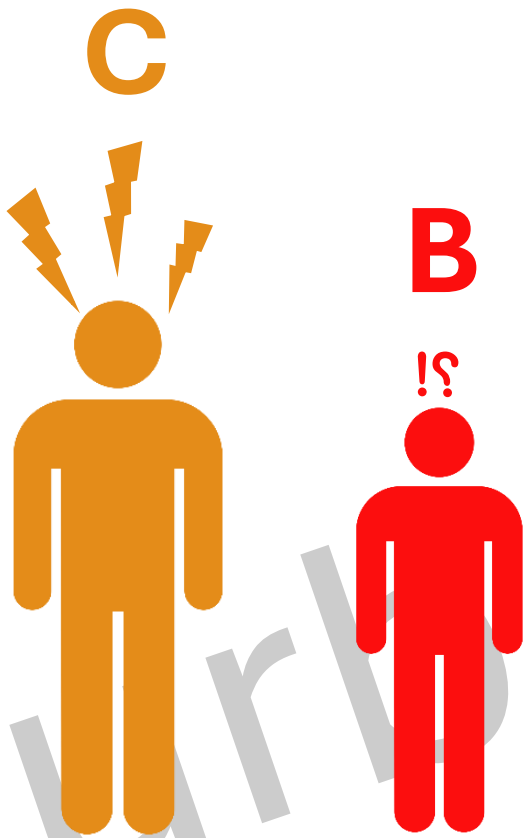


سناریو انتقال دارایی (ادامه) - 4

خب حالا که با مفهوم امضای دیجیتال آشنا شدیم میدونیم که A پول خودش رو امضا میکنه و به B میفرسته تا هنگام انتقال از B به C ، C بتونه با خیال راحت دارایی رو بگیره و کالا رو تحویل B بده .

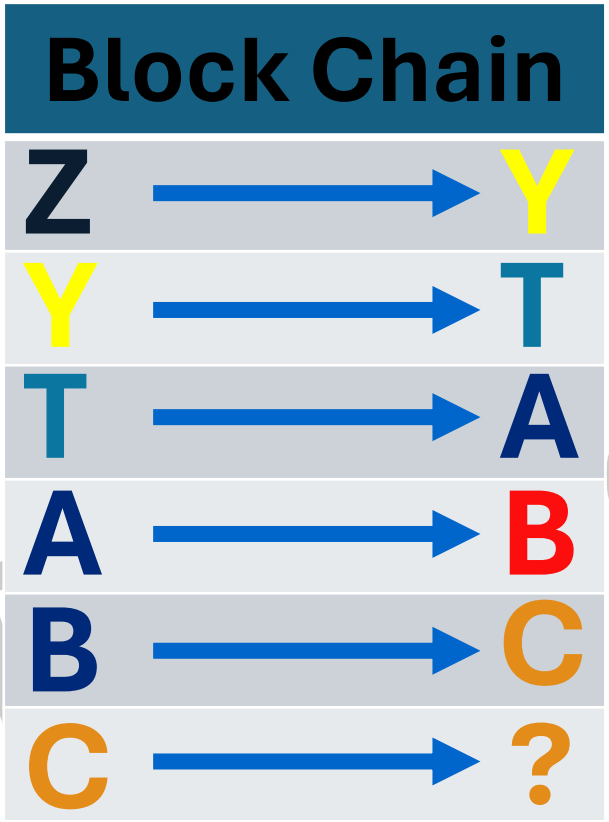


سناریو انتقال دارایی - 5



- اینجا باز دوباره C به B شک میکنه و میگه از کجا معلوم این پولی که داری بهم میدی رو جای دیگه خرج نکرده باشی ؟ یعنی همزمان هم به من ارسال کرده باشی و هم به مثلا F ؟؟؟؟؟
- بنظر شما چه راهکاری وجود داره که B بتونه اثبات کنه این کار رو نکرده ؟!

سناریو انتقال دارایی (Double spending) - 6



اینجا بلاکچین برای حل این مشکل (مشکل Double spending) به کمک ما میاد و با استفاده از ثبت اطلاعات بصورت دائمی و غیر قابل تغییر در بلاکچین (که در فصل ۱ بصورت مفصل راجبش حرف زدیم) میتونیم کاملا تاریخچه انتقال پول رو بررسی کنیم تا یک پول رو کسی دوبار خرج نکرده باشه !

جمع بندی

- ما برای ارسال پیام (تراکنش ها و دسترسی به دارایی) نیاز داریم تا از کلید عمومی و کلید خصوصی استفاده کنیم .
- کلید عمومی و خصوصی یک رشته بیتی هستند که توسط یک تابع ساخته می شوند :

Generate Key (Entry size) = (K_s و K_P)

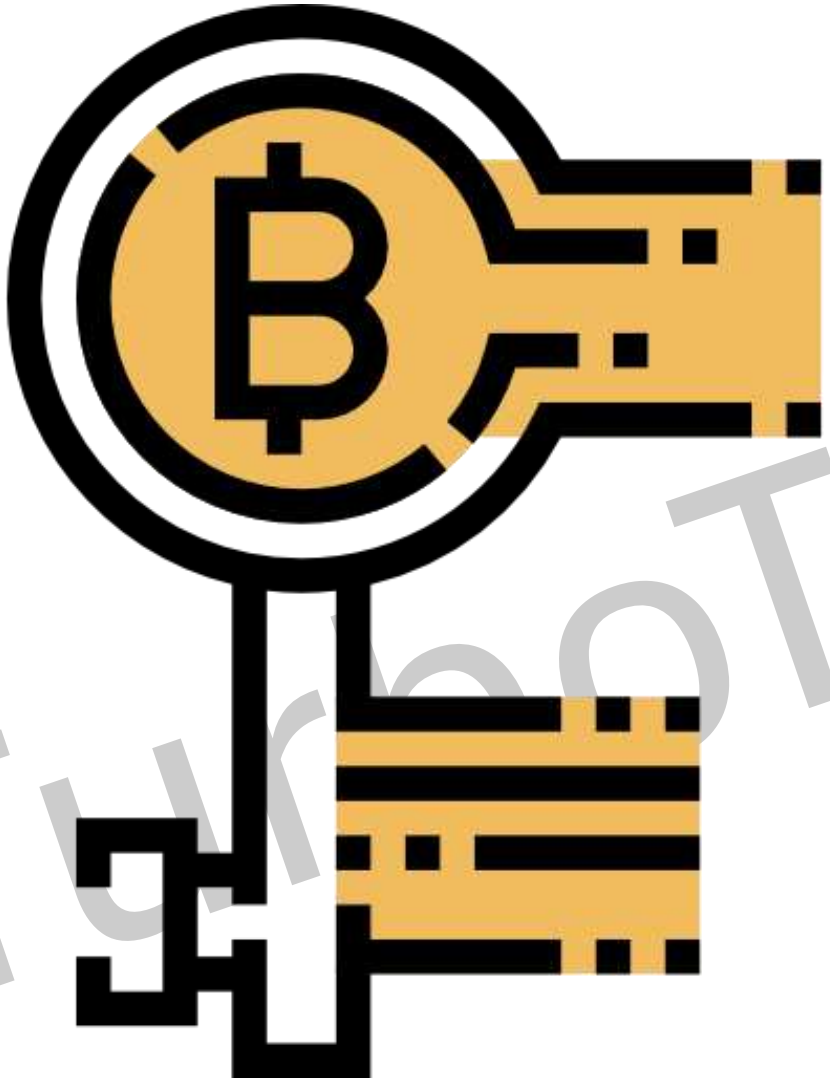
Output

- برای احرازهویت پیام ارسالی باید اون رو امضا کنیم (Signature) که به این منظور از Digital Signature کمک میگیریم.
- به منظور امضای پیام با استفاده از امضای دیجیتال از تابع زیر استفاده میکنیم :

Generate Signature (Message, K_s) = Digital Signature

- نود های شبکه برای تشخیص اعتبار پیام که از گیرنده واقعی ارسال شده باشه ، با استفاده از کلید عمومی پیام رو اعتبار سنجی میکنند :

Valid Message (Message , Sig , K_p) = Valid or not Valid



بررسی کلید خصوصی

PRIVATE KEY

کلید خصوصی چیست ؟

کلید خصوصی یک رشته متنی (Text string) ، به صورت ترکیبی از حروف و اعداد هست، که بطور کلی برای دسترسی به دارایی‌های شما بکار میره .

آیا میتونیم کلید خصوصی دیگران رو حدس بزنیم ؟

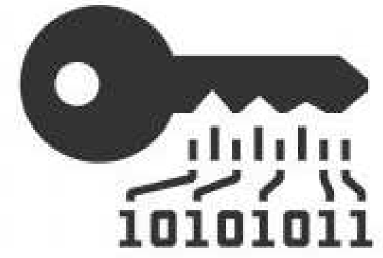
Private Key

SECRET

L2QpQtoqPYDSBAfTQqWKWNfzxsp6cZteZeG5QSvTgMbVRY1kjj5d

مدرس : مهندس فرشید میرزائی

کلید خصوصی چیست ؟ در ابتدا از کجا ساخته میشه ؟!



Generate Key (Entry size) = (K_S , K_P)

Binary:
1101110101010001000100111111110110111101101011000111000111001010100
0000001110011001010111011110010110000100111011110111010011101111011101
101111101011100011101011010111011000011011001101110100110011011100011
1001100010100110110000001011101001001011001101

- کلید خصوصی یک عدد تصادفی **۲۵۶ بیتی** هست که هنگام ساختن کیف پول ایجاد میشه .
  - به عبارتی اگر شما ۲۵۶ تا ۰ و ۱ رو بصورت تصادفی پشت سر هم بنویسید یک کلید خصوصی ایجاد کردید .
    - میتونید برای ایجاد کلید خصوصی (در حالت بیتی) ، سکه بندازید .
  - نرم افزار هایی هستند که برای شما این عدد تصادفی رو ایجاد میکنند (ولت ها ، شبیه ساز ها و ...) و ادامه فرآیند اون رو انجام میدن اما با این حال خودتون مایل هستید این کار رو انجام بدید ؟
    - اگر خودتون این کار رو انجام بدید میتونید مطمئن باشید که دیگه هیچ کس کلید خصوصی شمارو نمیدونه!

آیا میتونیم کلید خصوصی دیگران رو حدس بزنیم ؟

- حدس زدن یک کلید خصوصی (که به معنای دسترسی به دارایی یک شخص هست) یعنی : یک نفر یک رشته ۲۵۶ بیتی تصادفی رو نوشته و ما باید دقیقا اون عدد رو بنویسیم !!! راه حل چیه ؟

- برای حدس زدن یک کلید خصوصی از نظر علم آمار و احتمالات باید تمام زیرمجموعه های یک رشته ۲۵۶ بیتی رو محاسبه کنیم و تک تک اونها رو امتحان کنیم .

آیا میتونیم کلید خصوصی دیگران رو حدس بزنیم ؟

تعداد زیر مجموعه های یک مجموعه ی ۲۵۶ عضوی برابر است با :

$$2^{256}$$

۲ به توان ۲۵۶ مانند ۲ به توان ۳۲ است که ۸ بار در خودش ضرب شده باشد. ۲ به توان ۳۲ را می‌توان ۴ میلیارد در نظر گرفت؛ اکنون آن را ۸ بار در خودش ضرب کنید.

2^{256} =

115,792,089,237,316,195,423,570,985,008,687,907,853,269,984,665,640,564,039,457,584,007,913,129,639,936

آیا میتونیم کلید خصوصی دیگران رو حدس بزنیم ؟

- تخمین زده میشه ، کل جهان هستی که میگن قطری در اندازه ۹۳ میلیارد سال نوری داره ! دارای $۱۰^{۷۸}$ تا $۱۰^{۸۲}$ ذره ی اتم باشه .

- پس احتمالا حدس زدن کلید خصوصی شما مثل این میمونه که شما روی یکی از اتم های سازنده ی کیهان دست بذارید و از یک نفر بپرسید من روی کدوم اتم دست گذاشتم ؟!؟

- عددی که در اسلاید قبل بدست آوردیم برابر با تقریبا $۱۰^{۷۷}$ هست .

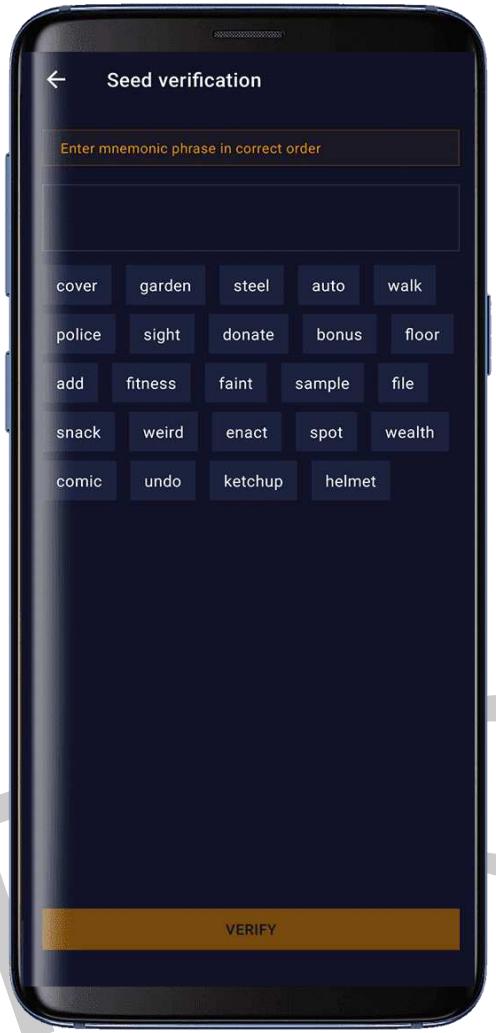
شکل نهایی کلید خصوصی – Base58

- اما شکل کلید خصوصی ای که ما در نهایت اون رو میبینیم بصورت ۰ و ۱ یا ۲۵۶ بیتی نیست ! و به این صورت هست :

5KYZdUEo39z3FPrtuX2QbbwGnNP5zTd7yyr2SC1j299sBCnWjss

- آدرسی که مشاهده میکنید نمونه یک کلید خصوصی هست ، که بعد از کلی فرآیند (که با محاسبات پیچیده بدست میاد و نیازی به یادگیری اون ندارید .) ساخته میشه و بصورت Base58 به شما نمایش داده میشه .
- Base58 یک مدل نمایش کلید خصوصی هست که اون رو در مقابل Base64 بصورت خوانا تر در میاره !

عبارت بازیابی چیست؟

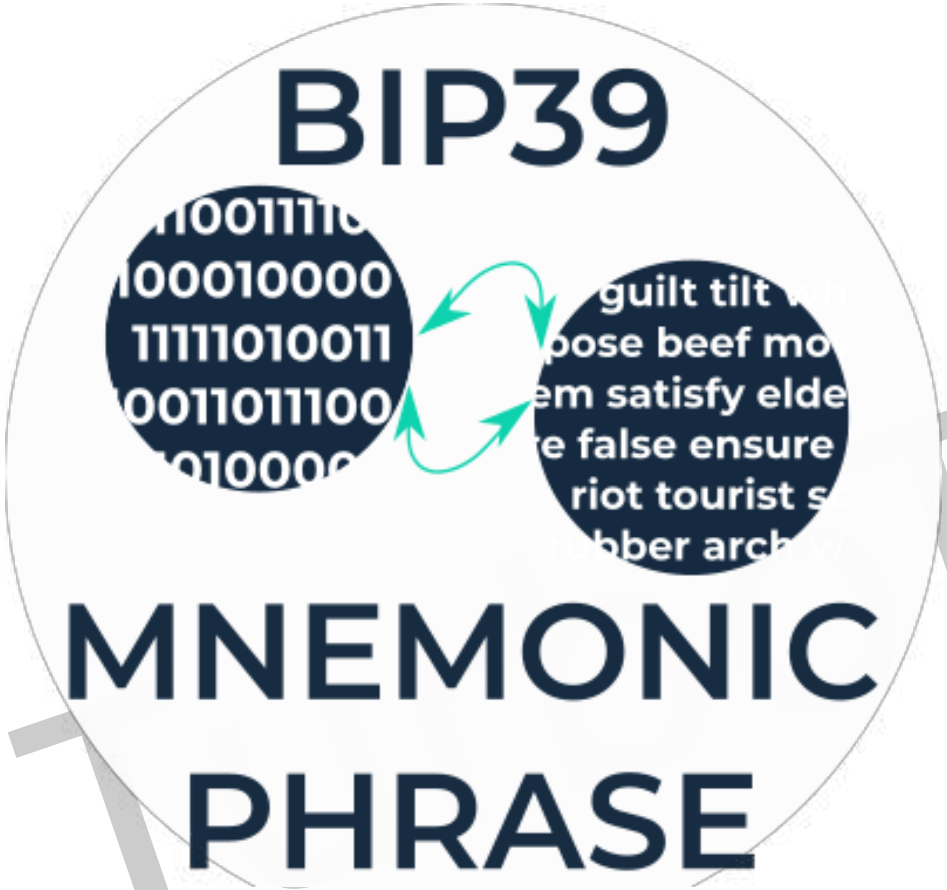


Mnemonic Phrase

- حالا که شکل نمایش کلید خصوصی رو متوجه شدیم بهتره با عبارات یادآور آشنا بشیم .

- بدلیل اینکه حفظ کردن کلید خصوصی و نگهداری اون کار مشکلی هست ، ایده عبارات یادآور توسط توسعه دهندگان بلاکچینی بوجود آمد ، که بطورخلاصه مجموعه ای از کلماتی هست که به‌عنوان راهی برای بازگردادن اطلاعات دسترسی به کیف پول استفاده میشه .

عبارت بازیابی چیست؟ BIP39



- طرح توسعه شماره ۳۹ بیت کوین(که یکی از طرح های توسعه بیتکوین هست) به کاربران ارز های دیجیتال کمک می‌کنه تا به وسیله کلمات مشخص و واضح که همون Mnemonic Phrase هست ، کلید اصلی و مخفی کیف پول خودشون رو ایمن کنند .

عبارت بازیابی چیست؟ Mnemonic Phrase

- نمونه کلید خصوصی :

5KYZdUEo39z3FPrtuX2QbbwGnNP5zTd7yyr2SC1j299sBCnWjss

❑ از اونجایی که به خاطر سپردن رشته کاراکترهای بالا کار دشواری هست،
Mnemonic Phrase به عنوان جانشین اون‌ها مطرح شدند.

- نمونه‌ای از عبارت بازیابی ۱۲ کلمه‌ای:

guilt tilt whip oppose beef movie bulk problem satisfy elder sentence sphere

طرح توسعه BIP39

BIP39 :

- در این طرح بیان شده که یک عبارت یادآور میتونه مجموعه ای از ۱۲ تا ۲۴ کلمه (باتوجه به آنتروپی اولیه ساخت اون که حداقل ۱۲۸ و حداکثر ۲۵۶ بیت هست) باشه .

- این عبارات از دل یک دیکشنتری ۲۰۴۸ کلمه ای بیرون آمده که در BIP39 مطرح شده .

Bitcoin
Improvement
Proposal

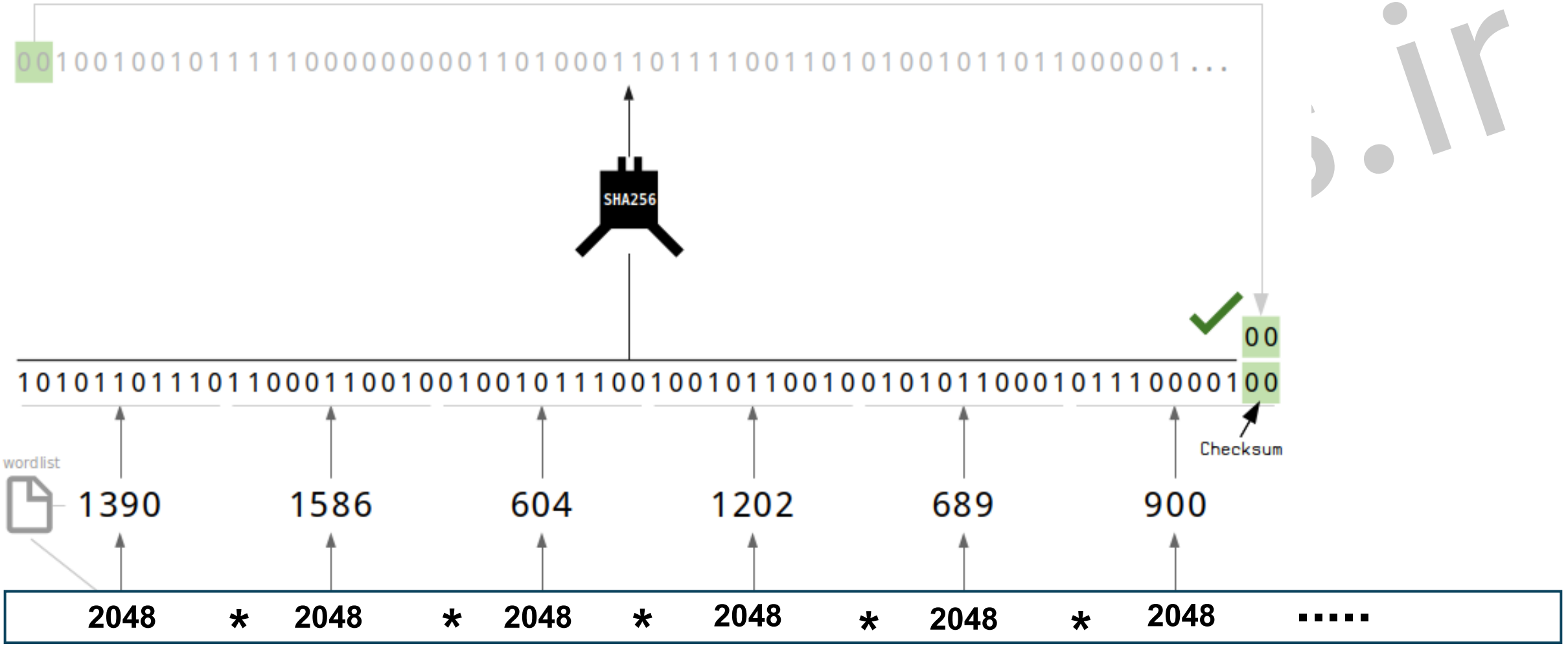
طرح توسعه BIP39

BIP39 :

- این عبارت در واقع یک عدد هست که به هر عدد ، یک کلمه از این دیکشنری اختصاص داده شده .
- اولین مجموعه ای که این استانداره رو پیشنهاد داد ، شرکت ساتوشی لبز بود
- آیا میتونیم عبارت یادآور رو حدس بزنیم ؟

1-128		2035	wrestle
1	**abandon**	2036	wrist
2	ability	2037	write
3	able	2038	wrong
4	about	**2039**	**yard**
5	above	2040	year
6	absent	2041	yellow
7	absorb	2042	you
8	abstract	2043	young
9	absurd	2044	youth
10	abuse	**2045**	**zebra**
11	access	2046	zero
		2047	zone

حدس زدن عبارت یادآور ...

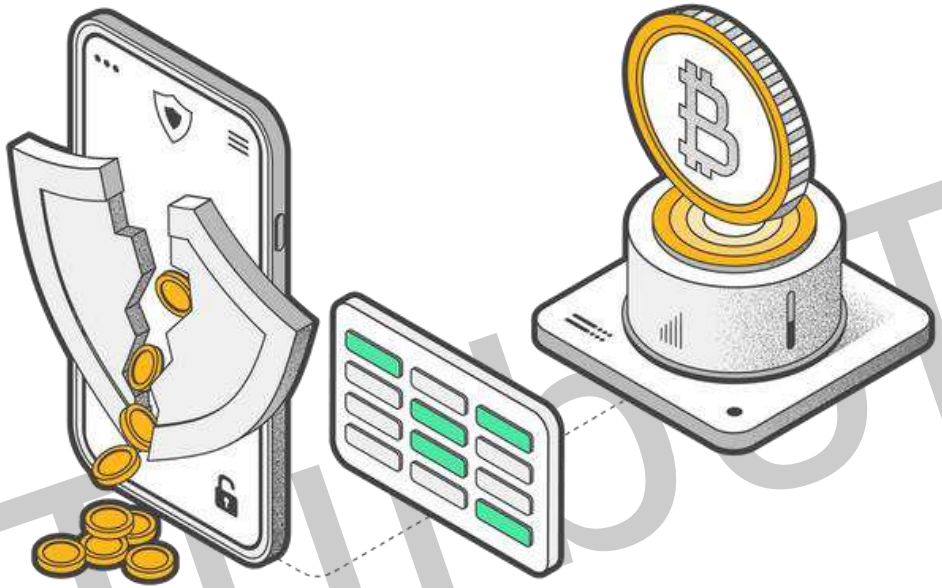


مدرس : مهندس فرشید میرزائی

بررسی کلید عمومی

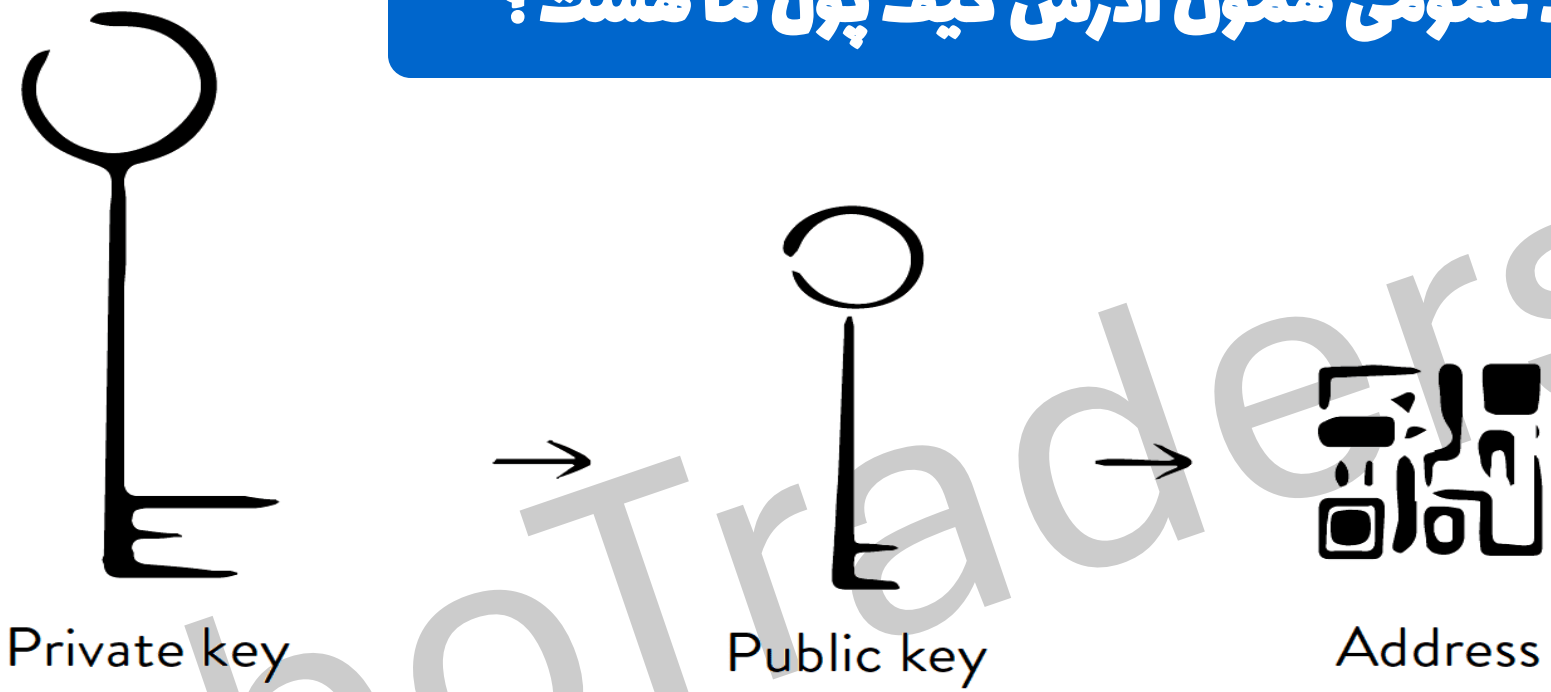
PUBLIC KEY

کیف پول ارز دیجیتال



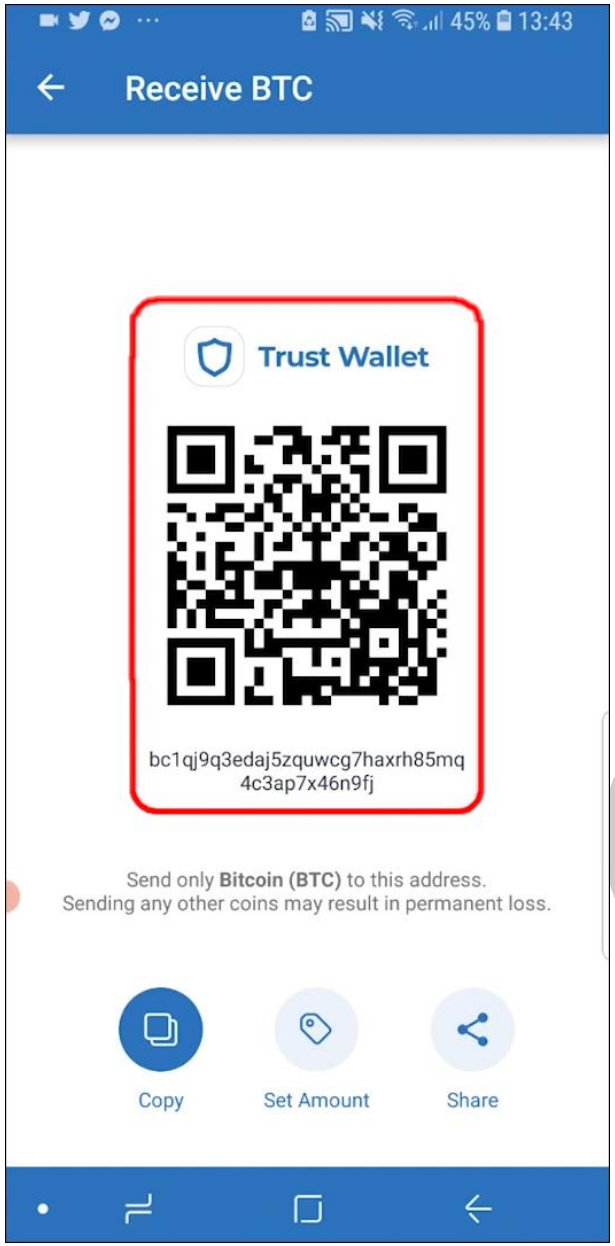
- کیف پول ارزهای دیجیتال، محلی برای نگهداری رمز ارز های شما نیست.
- دارایی های شما در بلاکچین نگه داری می شوند و این کیف پول ها فقط کلید های عمومی و خصوصی شما رو برای دسترسی به بلاکچین مدیریت و کنترل می کنند .

آیا کلید عمومی همون آدرس کیف پول ما هست ؟



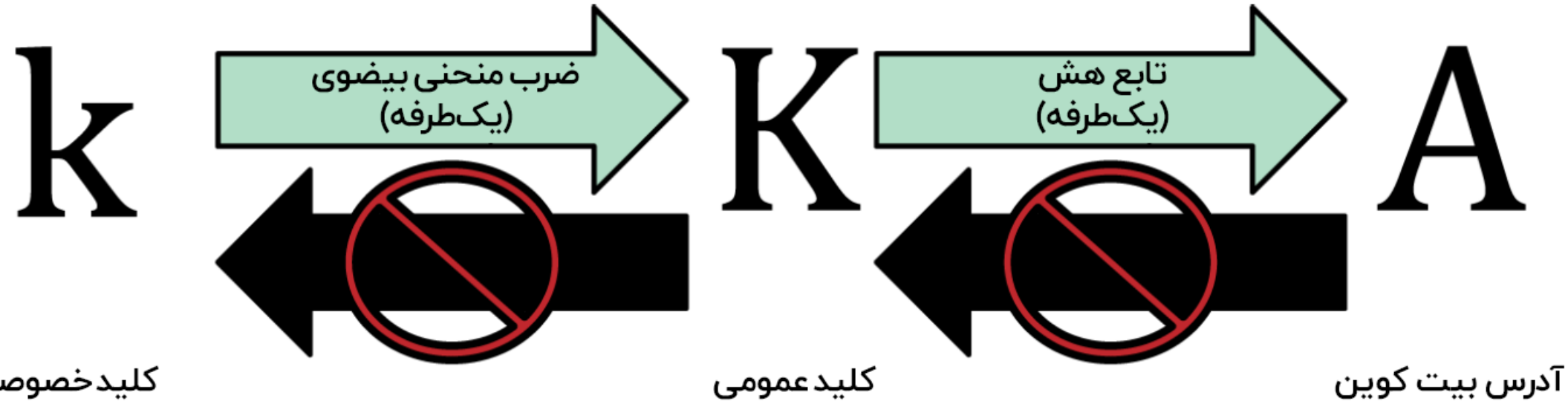
کلید عمومی از کلید خصوصی مشتق میشه و نهایتا برای ایجاد آدرس کیف استفاده میشه .کلید عمومی در امضای دیجیتالِ یک تراکنش استفاده میشه تا شبکه بتونه استفاده از کلید خصوصی برای تراکنش رو تایید کنه . و اینطوری کلید خصوصی فاش نمیشه .

منظور از آدرس کیف پول ارز دیجیتال چیست؟



آدرس کیف پول در واقع رشته‌ای از اعداد و حروف هست که می‌تونین اون رو با بقیه به اشتراک بگذارین تا به اون رمزارز بفرستن . آدرس‌ها از کلیدهای عمومی با استفاده از توابع هش یک‌طرفه به دست میاد ؛ به عبارتی امکان ایجاد کلیدهای عمومی از طریق داشتن آدرس‌ها وجود نداره.

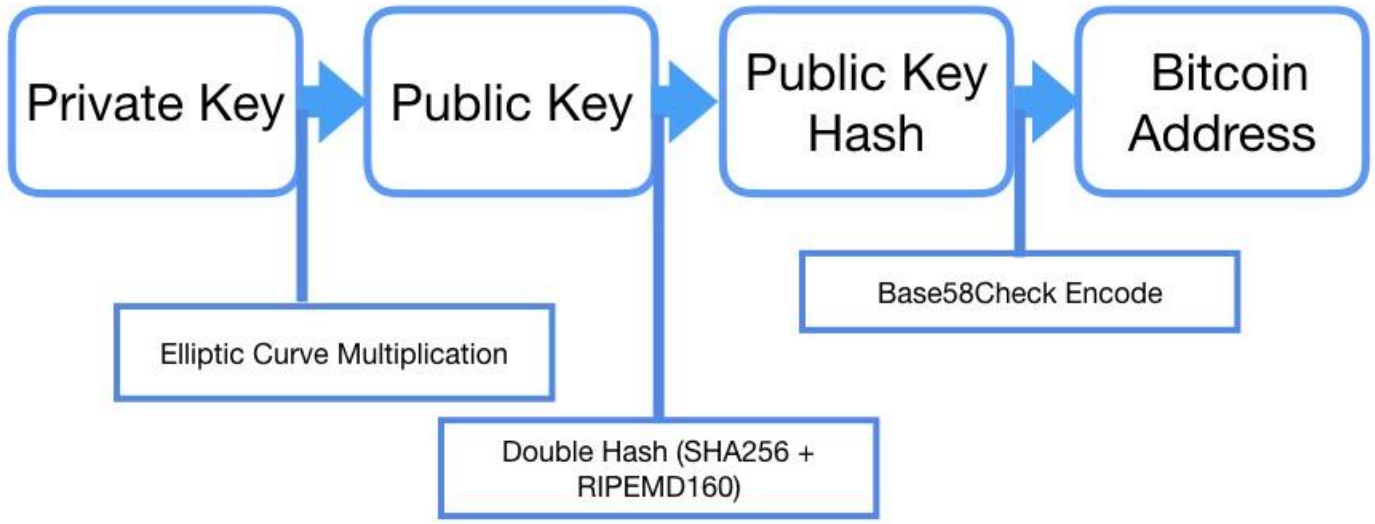
تفاوت کلید عمومی و آدرس کیف پول



در تصویر بالا میبینید که طی یک الگوریتم هش یا تابع هش آدرس کیف پول بیت کوین از کلید عمومی بدست میاد .

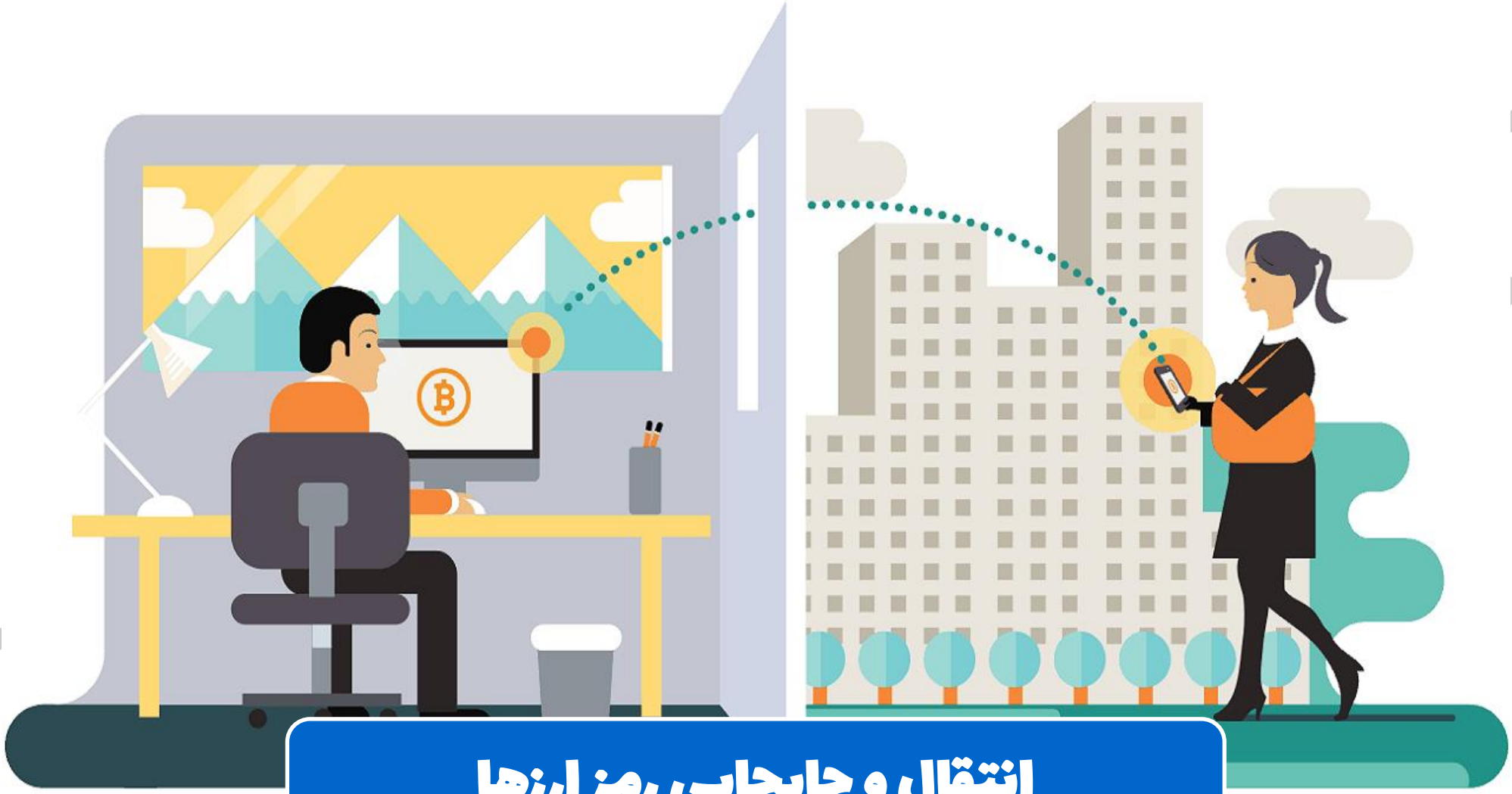
تفاوت آدرس کیف پول و کلید عمومی

ایجاد کلید عمومی از کلید خصوصی و ایجاد آدرس کیف پول از کلید عمومی در طی یک فرآیند یک طرفه



- پس آدرس کیف پول ها و کلید های عمومی با هم فرق میکنه و نباید اونها رو با هم اشتباه بگیریم .

- کلیدهای عمومی در تراکنش‌ها همراه با امضای دیجیتال به شبکه مخابره میشن تا صحت امضا و اطمینان از درستی کلید خصوصی مربوط به آدرس بیت کوین مورد نظر رو تایید بکنند .



انتقال و جابجایی رمز ارزها

مدرس : مهندس فرشید میرزائی

شبکه انتقال و پارامتر های مهم آن

برای درک بهتر مفهوم شبکه انتقال فرض کنید برای ارسال یک مرسوله پستی سه راه هوائی ، ریلی و زمینی رو برای انتقال دارید .

1

2

3

مدرس : مهندس فرشید میرزائی

شبکه انتقال و پارامتر های مهم آن

در مقایسه این سه راه به سه پارامتر مهم می رسیم :

1 - میزان کارمزد :

- میزان کارمزد در کدوم روش بیشتر هست ؟

2 – سرعت:

- سرعت انتقال در کدوم روش بیشتر هست ؟

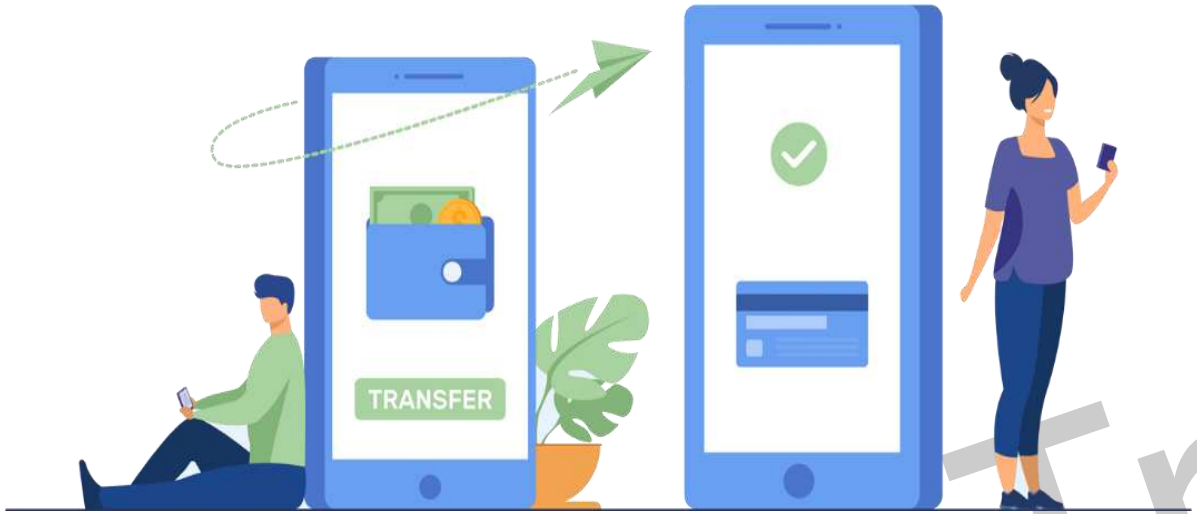
3 – پشتیبانی مقصد از شبکه انتقال :

- آیا شخص گیرنده امکان دریافت مرسوله رو از روش مورد نظر شما داره ؟ مثلا کسی که در شهرش فرودگاه نیست امکان دریافت مرسوله از طریق هوائی رو نداره !

یادآوری

- در اسلاید های قبل گفتیم که کوین (Coin) بلاکچین اختصاصی خودشو داره ولی توکن (Token) بلاکچین اختصاصی خودشو نداره و بر بستر بلاکچین های دیگه فعالیت میکنه .
- به عنوان مثال توکن تتر بر روی شبکه های اتریوم و ترون که هرکدوم یک کوین هستن و شبکه اختصاصی خودشون رو دارن قابل انتقال هست .

شبکه انتقال و پارامتر های مهم آن



- به دلیل اینکه هر شبکه بلاک چین ، قوانین و پروتکل‌های مخصوص به خودش رو داره ، انتقال رمز ارز در اونها براساس سه پارامتری که گفتیم فرق میکنه .

- به عنوان مثال انتقال رمز ارز تتر بر بستر شبکه ترون (TRC20) کارمزد کمتر و سرعت بیشتری نسبت به شبکه اتریوم (ERC20) داره . به همین جهت موقع انتقال یک رمز ارز به کیف پول شخص دیگه باید به شبکه انتقال اون دقت کنیم .

اشتباهات رایج - اشتباه در انتقال

- یکی از رایج‌ترین اشتباهات ، ارسال رمز ارز به یک آدرس ناشناس هست .
- برای مثال فرد ممکنه از بین آدرس‌های قدیمی که هنگام ارسال رمز ارز استفاده کرده ، یک آدرس اشتباه رو انتخاب کنه و ارز خودش رو به اون ارسال کنه. با این کارارز از دسترس شما خارج می شه و احتمال بازیابی اون نزدیک به صفر هست. تنها در صورتی بازگردانی این ارز ممکنه که صاحب آدرس کیف پول مقصد را پیدا کنین و اون نیز بپذیره که ارز را برگردونه.

اشتباهات رایج - ارسال ارز به شبکه بلاکچین اشتباه

یکی از اشتباهات رایج در انتقال رمز ارزها ، عدم توجه به شبکه انتقال ارز مورد نظر هست ، گاها پیش میاد افراد بخاطر مشابه بودن فرمت آدرس کیف پول ها ، رمز ارزها رو در بستر بلاکچین اشتباه ارسال میکنن .

مدرس : مهندس فرشید میرزائی

تشخیص شبکه انتقال از روی آدرس گیرنده

همونطور که میدونید در بانک های ایران ، پیش شماره کارت های بانکی میتونه مشخص کنه که این کارت مربوط به کدوم بانک هست ، به عنوان مثال اگر کسی به شما شماره کارتی بده که پیش شماره ۶۰۳۷۹۹ داره شما میتونین براساس این پیش شماره بفهمید که این کارت مربوط به **بانک ملی ایران** هست .

تشخیص شبکه انتقال از روی آدرس گیرنده

BC1QAR0SRRR7XFKVY5L643LYDNW9RE59GTZZWF5MDQ

TWSVAB9EWAGKDUMTD7XOEDKVS7AOYVKGN7

0X5C6FB802F173DBA15E2CAADA433032B1368AF59F

در شبکه های انتقال بلاکچین رمز ارزها هم ساختاری مشابه این ساختار وجود داره و آدرس کیف پول ها بر بستر هر شبکه انتقال پیشوندی مشخص دارن و شما باید در هنگام انتقال دارایی به یکی بودن **پیشوند آدرس** و **پشتیبانی شبکه انتقال در طرف مقابل** حتما دقت کنید.

تشخیص شبکه انتقال از روی آدرس گیرنده

0x4900584a78ecf54D3511c5707cF46f1b54096F03

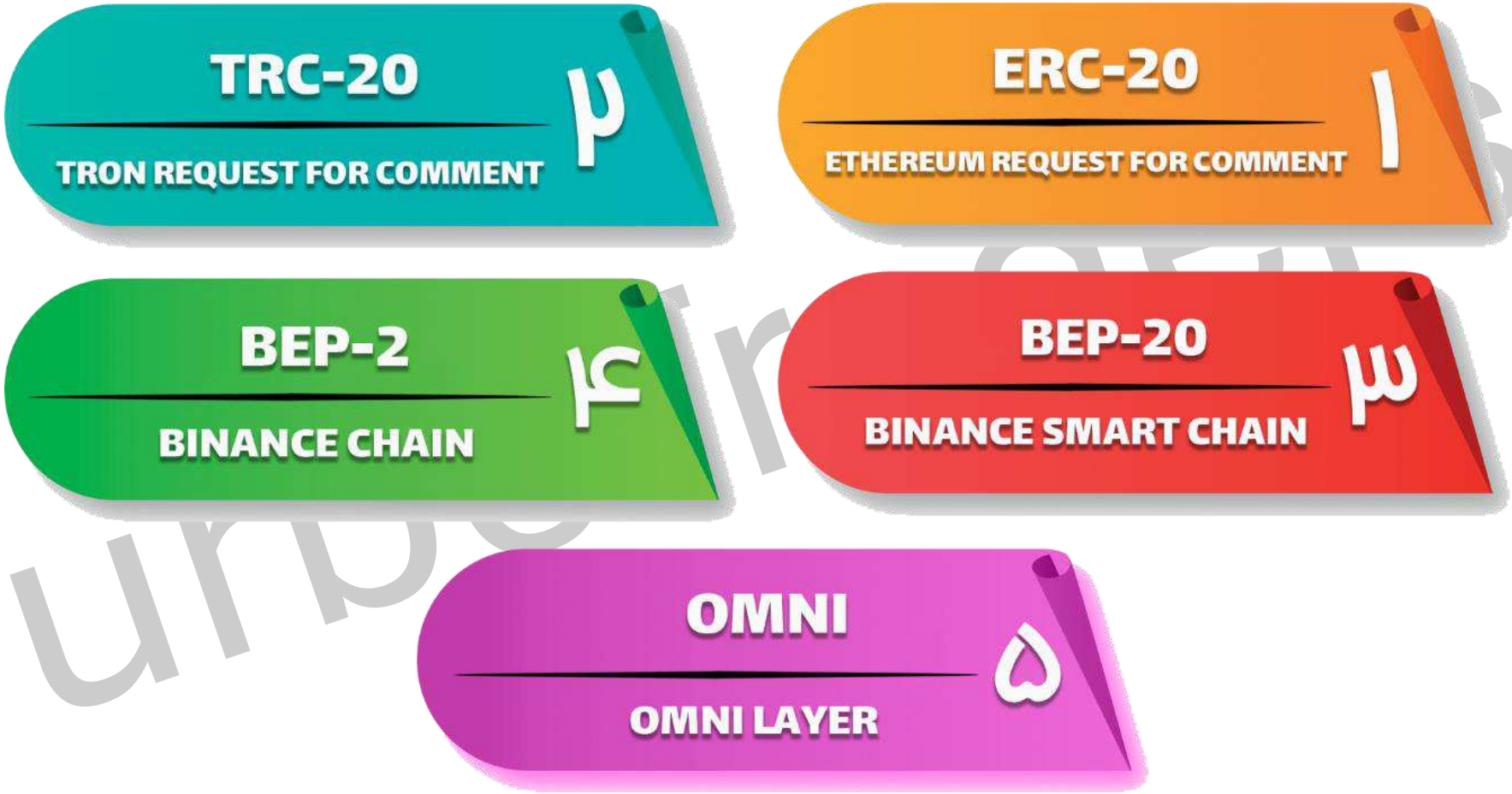
0x4900584a78ecf54D3511c5707cF46f1b54096F03

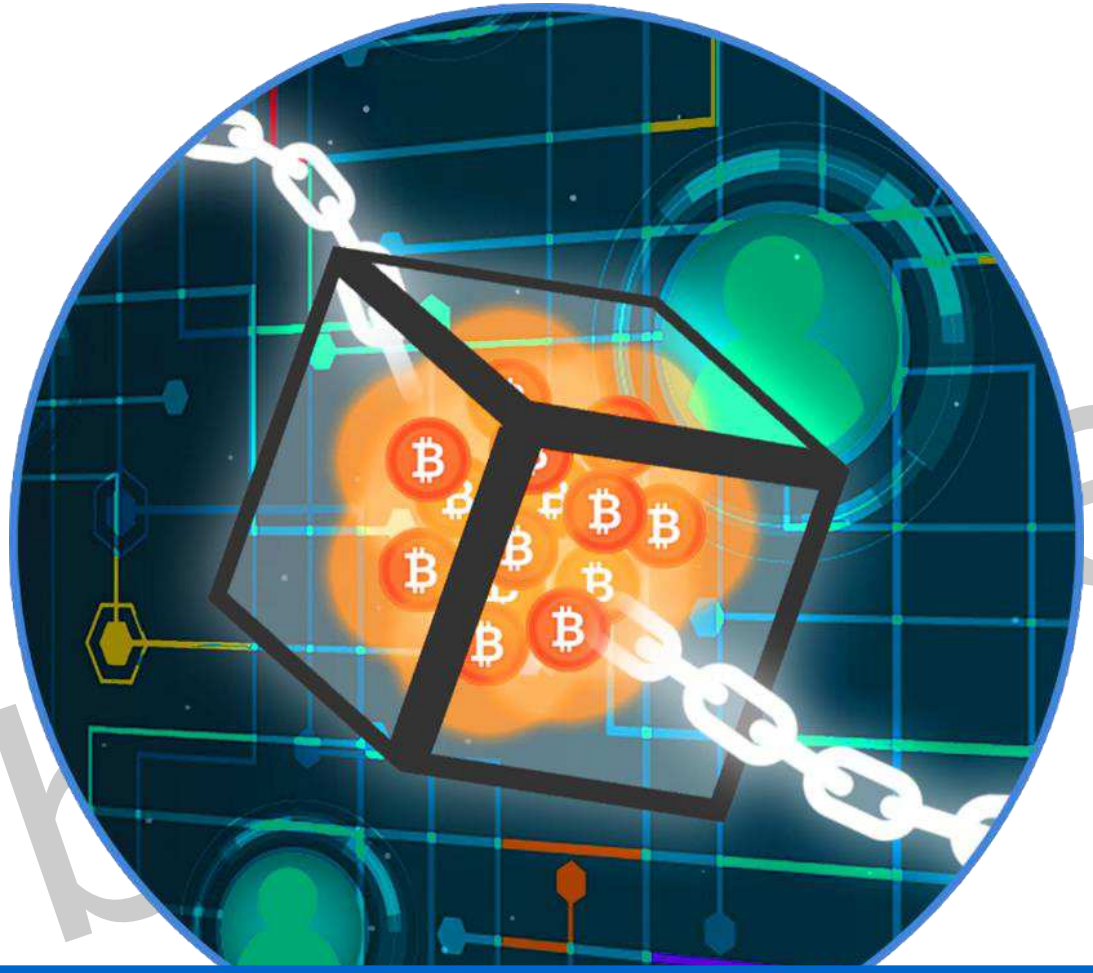
BEP-20

ERC20

در بعضی موارد استثناء به دلیل استفاده از الگوریتم رمزنگاری مشترک و یکسان بودن آدرس کیف پول ها ، پیشوند های آن ها هم یکسان هستند ، مثلا آدرس توکن ها بر بستر شبکه اتریوم (ERC20) و بایننس اسمارت چین (BEP-20) هردو با 0X شروع میشن ، یا پیشوند آدرس کیف پول شبکه پالیگان با اتریوم برابر هست . در چنین مواردی باید با هماهنگی بین فرستنده و گیرنده از صحت درستی کیف پول گیرنده ، اطمینان حاصل کرد .

پنج مورد از مهم ترین شبکه های انتقال رمزارزها

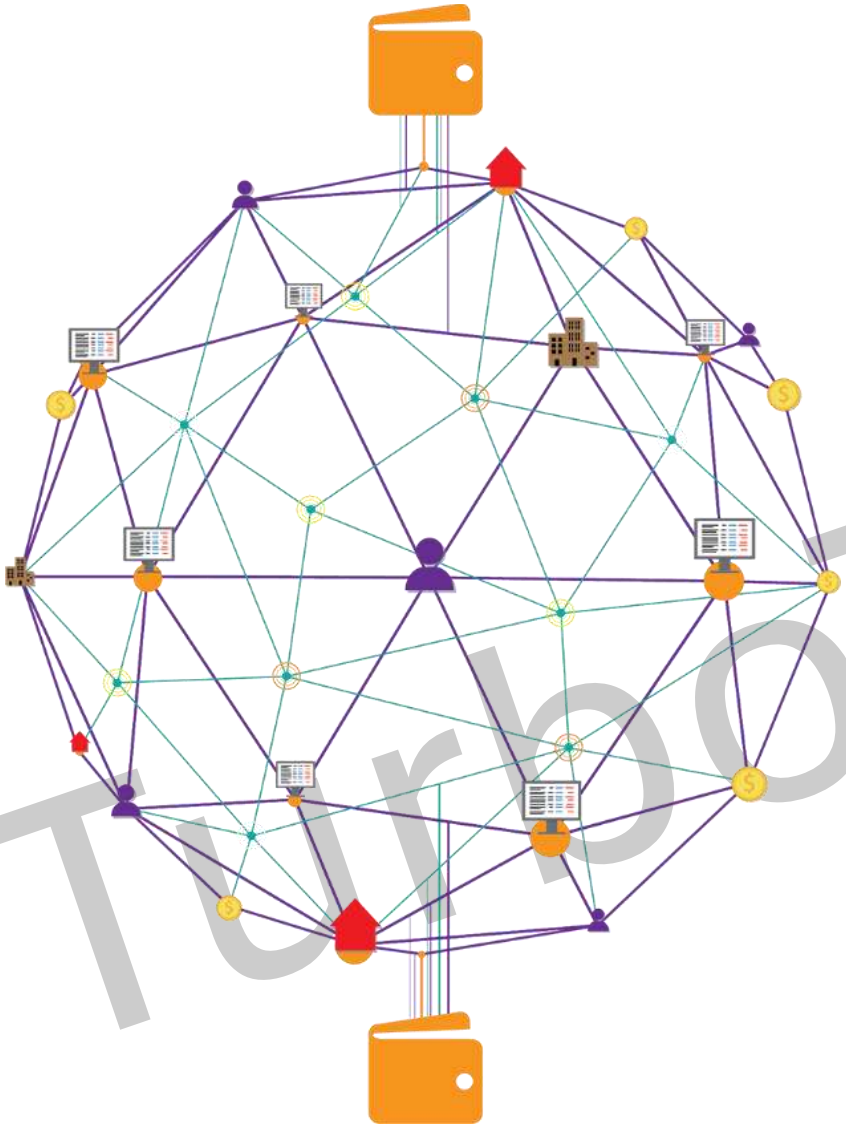




انتخاب درست شبکه انتقال

مدرس : مهندس فرشید میرزائی

مقدمه



دراسلاید های قبل در مورد شبکه های انتقال و نکات مربوط به اون صحبت کردیم ، در این بخش میخوایم با ۶ مورد از رایج ترین شبکه های انتقال و ویژگی های اون ها بیشترآشنا بشیم تا در موقع انتقال رمز ارز از کیف پول یا صرافی ، مناسب ترین شبکه انتقال رو انتخاب کنین .

پارامترهای انتخاب شبکه انتقال

1 پشتیبانی مقصد

پشتیبانی مقصد از شبکه انتقال مورد نظر شما، نکته ای هست که حتما در انتقال رمز ارز باید به اون توجه داشته باشید .

2 سرعت

سرعت و مدت زمان انتقال یک رمز ارز از مهم ترین پارامتر های انتخاب یک شبکه انتقال هست .

3 کارمزد

میزان کارمزدی که برای انتقال یک رمز ارز از یک کیف پول به کیف پول دیگه پرداخت میشه . معیاری برای انتخاب یک شبکه انتقال محسوب میشه .

مدرس : مهندس فرشید میرزائی

نگاه کلی به ده شبکه انتقال رایج

	نام شبکه	نوع بلاکچین	کارمزد	سرعت	پیشوند آدرس ولت
1	ERC20	ETHEREUM	وابسته به شلوغی شبکه	وابسته به شلوغی شبکه	ابتدا با 0X
2	TRC20	TRON	کم	بالا	ابتدا با T
3	BITCOIN	BITCOIN	بالا	کم	ابتدا با ۱ یا ۳ یا BC1
4	OMNI	OMNI LAYER	بالا	کم	ابتدا با ۱ یا ۳ یا BC1
5	BEP-2	BINANCE (BNB)	کم	بالا	ابتدا با BNB
6	BEP-20	BSC	کم	بالا	ابتدا با 0X

مدرس : مهندس فرشید میرزائی

نگاه کلی به ده شبکه انتقال رایج

نام شبکه	نوع بلاکچین	کارمزد	سرعت	پیشوند آدرس ولت
7 POLYGON	POLYGON	کمتر از اتریوم	بالا	ابتدا با 0X
8 DASH	DASH	کم	بالا	ابتدا با X
9 LITECOIN	LITECOIN	کم	بالا	ابتدا با L یا l
10 DOGECOIN	DOGECOIN	کم	بالا	ابتدا با D

توجه داشته باشید که این ده شبکه ، فقط بخشی از شبکه های انتقال موجود در بازارکریپتوکارنسی می باشد

شبکه انتقال اتریوم - ERC 20

پیشوند آدرس کیف پول ها در شبکه انتقال اتریوم

0X513BFDEBC2B86B67CA4E56FDB00CEB051F3050B9

ERC 20 یک شبکه بلاکچین نسل دوم با ارز اتریوم هست . توکن های ایجاد شده روی شبکه **ERC 20** از شبکه اتریوم برای انتقال و انجام تراکنش های خودشون استفاده میکنن .کارمزد انتقال در این شبکه با استفاده از معیاری به نام **Gas fee** تعیین می شه که بنابر شلوغی شبکه کارمزد انتقال میتونه متغیر باشه به دلیل پشتیبانی این شبکه برای اولین بار از قراردادهای هوشمند این شبکه با مشکل مقیاس پذیری و شلوغی شبکه مواجه هست که باعث بالا رفتن کارمزد در انتقال های عادی شده .

ERC 20 چیست ؟

Ethereum Request for Comment

- استاندارد ERC-20 مجموعه‌ای از قوانینی هست که باید یک روی یک توکن اعمال بشه تا بتونه روی اکوسیستم اتریوم فعالیت کنه .

- توکن های ERC-20 بدلیل اینکه میتونن از قابلیت جذب سرمایه یا ICO بهره ببرن بسیار مهم و کاربردی هستن .

شبکه انتقال ترون - TRC 20

TRC 20 شبکه انتقال ارز ترون هست . و این شبکه انتقال، به سریع بودن و کارمزد پایین شناخته می شه . از توکن های معروف و پرکاربرد اون تتر با نماد **USDT** هست و از کم هزینه ترین شبکه انتقال برای تتر به شمار میاد به همین جهت عموما از این شبکه انتقال برای انتقال تتر استفاده میشه و در مقایسه با کارمزدهای پرداختی در شبکه **ERC 20** ، کارمزد اون بسیار کمتر هست.

شبکه انتقال بایننس - BEP2

پیشوند آدرس کیف پول ها در شبکه انتقال بایننس

BNB136NS6LFW4ZS5HG4N85VDTHAAD7HQ5M4GTKGF23

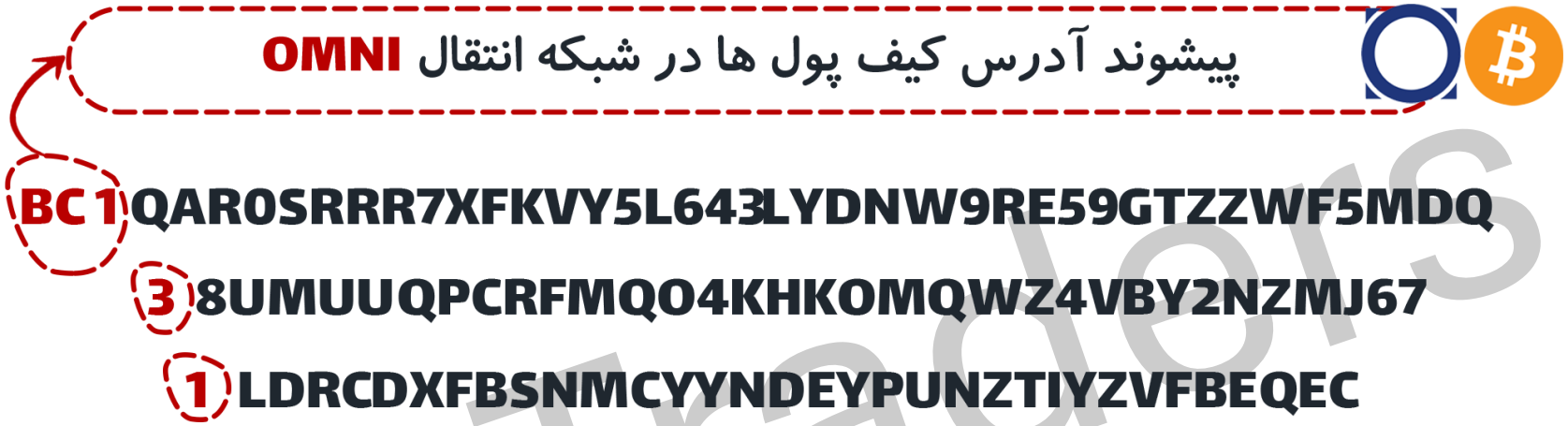
شبکه **BEP2** ، شبکه ای مربوط به بلاکچین صرافی بایننس هست . سرعت انتقال بالا و میزان کارمزد کم دو عامل متمایزکننده شبکه بلاک چین بایننس از دیگر شبکه هاست . اگر تصمیم دارید مبالغ پایین جا به جا کنید، این شبکه می تونه گزینه مناسبی برای این کار شما باشه.در حال حاضر کیف پول تراست ولت از شبکه BEP2 پشتیبانی می کنه.

MEMO نوعی برچسب انتقال هست که در زمان انتقال رمز ارز در این شبکه ، این برچسب رو هم ، همراه آدرس کیف پول مقصد ، باید از جانب گیرنده مطلع بشید و در کادر مربوطش وارد کنید .

شبکه انتقال بایننس اسمارت چین - BEP20

- شبکه **BEP20** هم توسط صرافی بایننس توسعه و ارائه شده. کارمزد و سرعت انتقال ارزهای دیجیتال در شبکه BEP20 ، نسبت به شبکه BEP2 مناسب تر هست .
- نماد این شبکه BSC - Binance Smart Chain هست و یکی از قابلیت های خوب این بلاکچین ، همخوانی با هر دو شبکه BEP2 و ERC20 هست. شبکه BSC با هدف پشتیبانی از قرارداد هوشمند ، تشکیل شده است.

پیشوند آدرس کیف پول ها در شبکه انتقال Omni



شبکه Omni یک لایه نرم افزاری هست که بر روی محبوب ترین بلاک چین جهان یعنی بیت کوین ساخته شده . به همین دلیل آدرس کیف پول این شبکه و تراکنش ها دقیقا مثل شبکه بیت کوین هستن.سرعت این شبکه پایین هست و همچنین کارمزد اون بسیار بالاست.لایه Omni در واقع در بالای بلاک چین بیت کوین توسعه داده شده است. امنی یک رمز ارز نیست ، بلکه لایه ای هست که ویژگی های مبادله پیشرفته مثل ایجاد ارز ، معاملات غیر متمرکز ، قراردادهای هوشمند و ... رو ارائه میده .

شبکه انتقال پالیگان - Polygon

پیشوند آدرس کیف پول ها در شبکه انتقال پالیگان

0X513BFDEBC2B86B67CA4E56FDB00CEB051F3050B9

شبکه پالیگان یکی از برترین پروژه های لایه دوم اتریوم هست که محبوبیت بالایی رو داره. با استفاده از Polygon و ارز ماتیک که ارز بومی پالیگان هست ، مشکلات مقیاس پذیری اتریوم قابل حل هستش و به همین دلیل تا میزان زیادی سرعت بیشتر و کارمزد کمتری نسبت به بلاکچین اتریوم داره . هدف نهایی شبکه polygon، کمک به توسعه ، امنیت و افزایش کارایی بلاکچین اتریوم هست تا از این راه توسعه‌دهندگان به ارائه محصولات جذابتر خود در مدتی کوتاه تشویق بشن.

شبکه انتقال دش - Dash

شبکه Dash از ویژگی‌هایی مانند تایید آنی تراکنش‌ها ، مقابله با دابل اسپندینگ و محافظت از حریم خصوصی کاربر بهره‌مند است و بر اساس یک مدل خودگردان فعالیت می‌کند.شبکه انتقال دش از سرعت و کارمزد خوبی برخوردار هست .

شبکه انتقال لایت کوین - LiteCoin

لایت کوین یکی از قدیمی‌ترین کوین‌های موجود در بازار کریپتوکارنسی هست . این رمزارز همتا به همتا شباهت‌های زیادی با بیت‌کوین داره ، هدف این پروژه افزایش سرعت و کاهش کارمزد تراکنش‌ها و افزایش سرعت استخراج بلاک‌هاست. این شبکه بیت کوین رو رقیب خودش نمی‌دونه . در واقع تیم سازنده اون ، بیت کوین رو وسیله‌ای برای حفظ ارزش در بلندمدت و لایت‌کوین رو برای معاملات روزانه و کم ، مناسب می‌دونه.

شبکه انتقال لایت کوین - LiteCoin

	بیت کوین	لایت کوین
سال ایجاد	۲۰۰۹	۲۰۱۱
خالق	ساتوشی ناکاموتو	چارلی لی
تعداد کوین‌ها	۲۱ میلیون	۸۴ میلیون
زمان ایجاد بلاک	۱۰ دقیقه	۲/۵ دقیقه
الگوریتم	اسکریپت	SHA-256
اولین پاداش ماینینگ	BTC ۵۰	LTC ۵۰
پاداش ماینینگ فعلی (مارس ۲۰۲۱)	BTC ۶/۲۵	LTC ۱۲/۵
زمان هاوینگ	هر ۲۱۰ هزار بلاک	هر ۸۴۰ هزار بلاک

شبکه انتقال دوج کوین - DogeCoin

شبکه دوج کوین یک شبکه غیرمتمرکز و متن‌باز برای پرداخت‌های آنلاین و انتقال‌های مالی با سرعت بالا و از طریق تراکنش‌های همتا به همتا (Peer To Peer) هست. بلاکچین این ارز می‌تونه حدود ۳۰ تراکنش در ثانیه رو پردازش کنه که بسیار بالاتر از بیت‌کوین هست. کوین‌ها در این پروژه از طریق فرایند استخراج تولید می‌شن به عبارت دیگه از الگوریتم اجماع که از نوع اثبات کار (Proof of Work) هست استفاده میکنند.

تنوع شبکه های انتقال در بازار رمزارزها

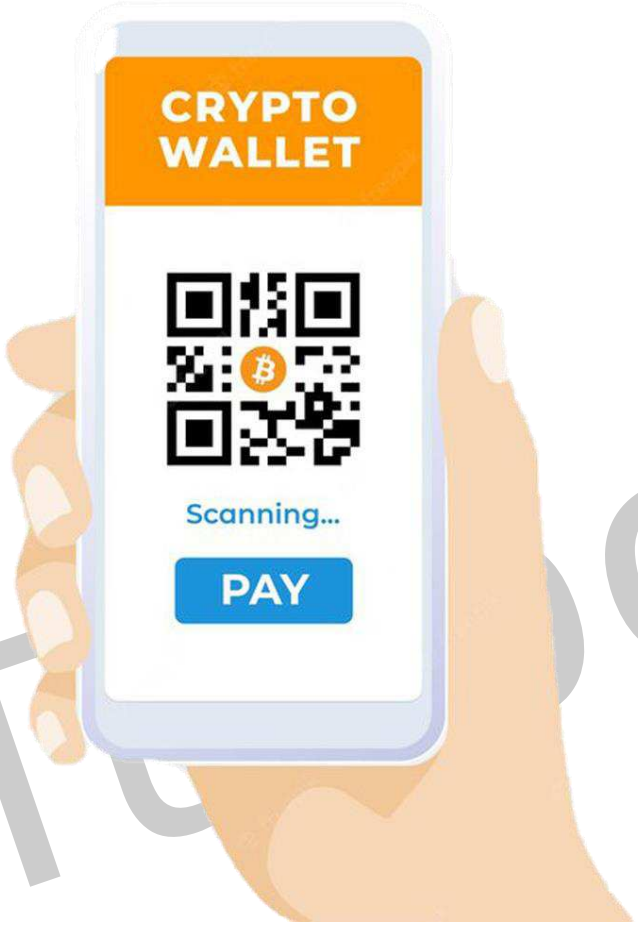
دقت داشته باشید که شبکه های انتقال
محدود به مواردی که گفته شد نیستند
و در اسلاید های قبل صرفا رایج ترین شبکه
های انتقال رو به شما معرفی کردیم

مدرس : مهندس فرشید میرزائی

انواع آدرس کیف پول در شبکه بیتکوین

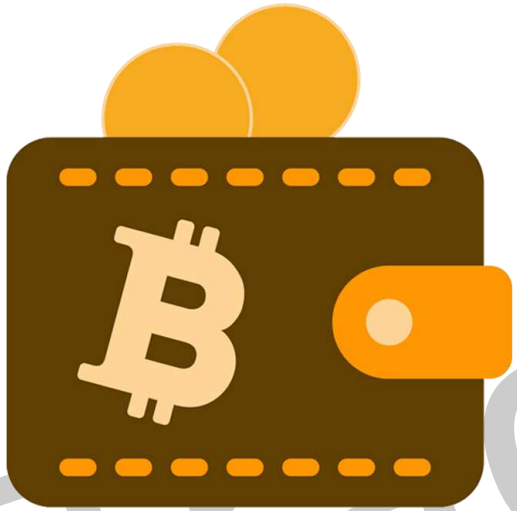
مدرس : مهندس فرشید میرزائی

مقدمه



در حال حاضر آدرس‌های شبکه اصلی بیت کوین دارای ۳ ساختار مختلف هستن. اکثر افراد فعال در حوزه کریپتوکارنسی، معمولاً از انواع آدرس بیت کوین در شبکه‌های بلاکچین برای انجام تراکنش‌ها استفاده می‌کنن که البته در تضاد با یکدیگه نیستن و باهم سازگارن. اما این رو بدونین که برای انتقال بیت کوین ، صرافی یا کیف مورداستفاده شما باید حداقل از یکی از انواع آدرس بیت کوین، پشتیبانی بکنه.

سه نوع فرمت آدرس در کیف پول های بیت کوین



1. P2PKH یا Legacy
2. P2SH یا Compatibility
3. BECH32 یا Segwit یا Default

آدرس P2PKH : Pay to Pubic Key Hash

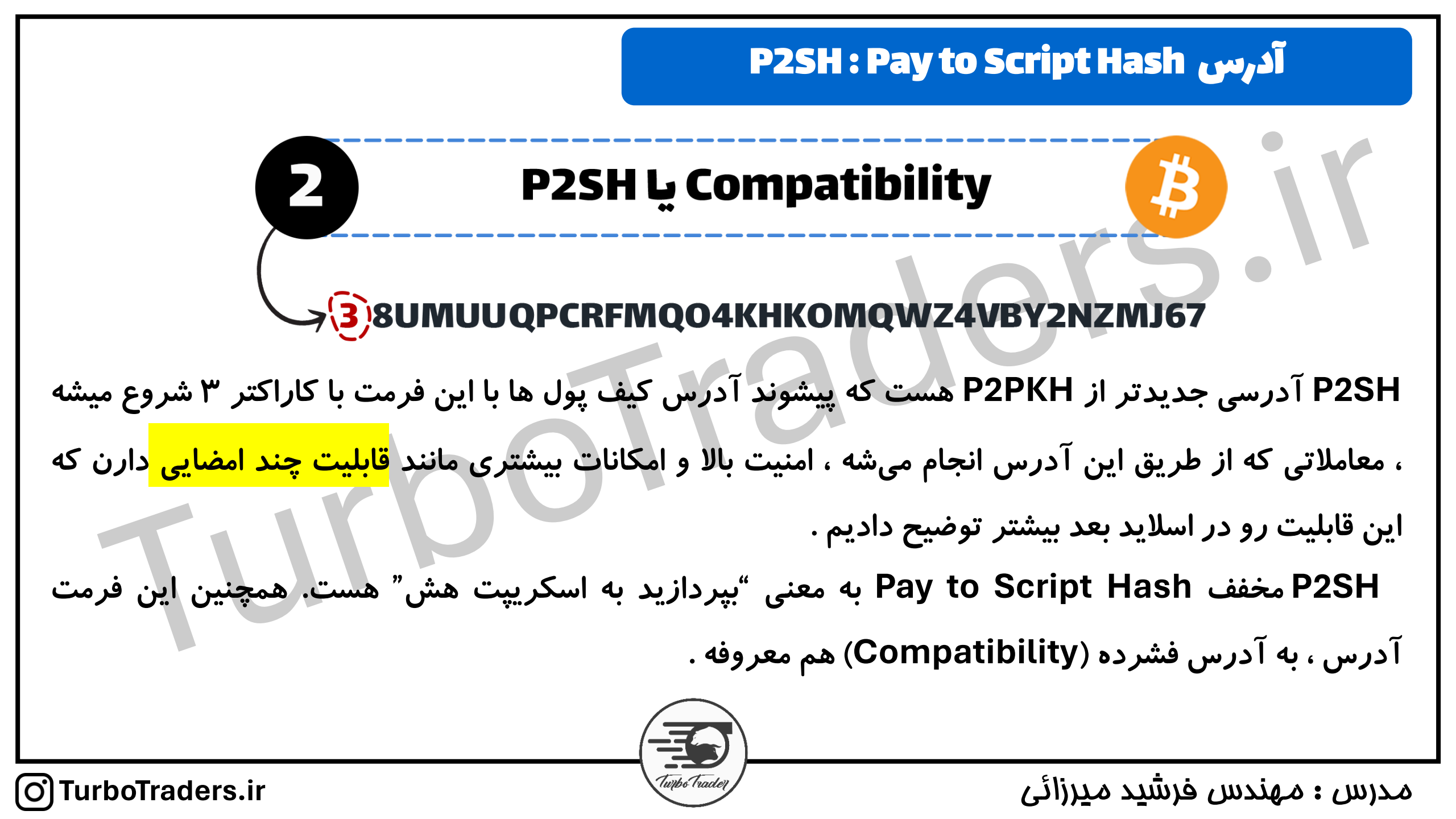
1 P2PKH یا Legacy

یکی از انواع آدرس های بیت کوین، فرمت آدرس P2PKH هست. این فرمت یکی از استانداردهای آدرس بیت کوین هست که پیشوند آدرس کیف پول ها با این فرمت با کاراکتر ۱ شروع میشه. همچنین این فرمت آدرس ، به آدرس لگسی (Legacy) یا میراثی هم معروف هست.دلیل این نامگذاری اینه که این فرمت اصلی ترین و اولین فرمت در شبکه بیت کوین هست .

P2PKH مخفف Pay To Pubic Key Hash هست. این عبارت به معنی "پرداخت کنید به هش کلید عمومی گیرنده" می باشد.

آدرس P2SH : Pay to Script Hash

2 P2SH یا Compatibility

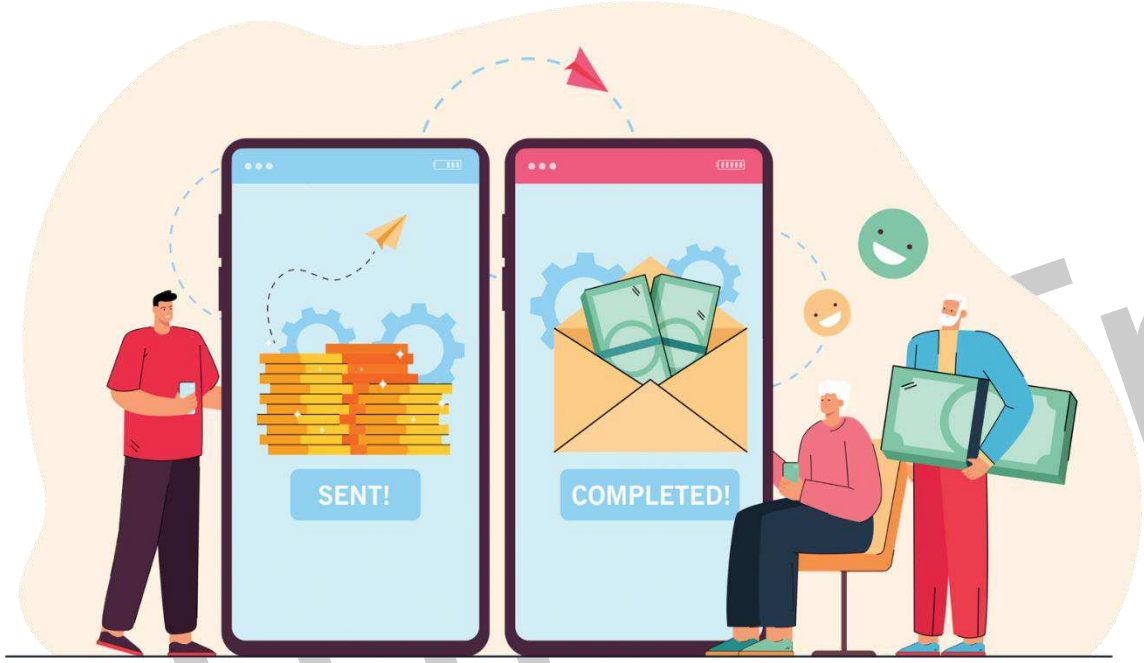


3 8UMUUQPCRFMQO4KHKOMQWZ4VBY2NZMJ67

P2SH آدرسی جدیدتر از P2PKH هست که پیشوند آدرس کیف پول ها با این فرمت با کاراکتر ۳ شروع میشه ، معاملاتی که از طریق این آدرس انجام می‌شه ، امنیت بالا و امکانات بیشتری مانند قابلیت چند امضایی دارن که این قابلیت رو در اسلاید بعد بیشتر توضیح دادیم .

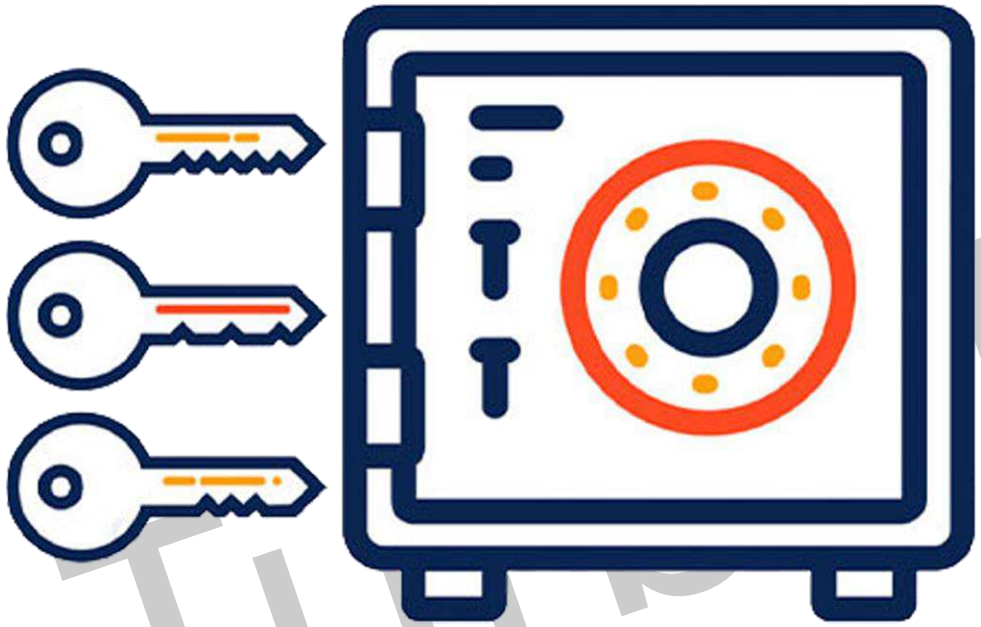
P2SH مخفف Pay to Script Hash به معنی “بپردازید به اسکریپت هش” هست. همچنین این فرمت آدرس ، به آدرس فشرده (Compatibility) هم معروفه .

قابلیت چند امضایی



فرض کنین زمان چند سال جلو رفته و دیگه خبری از پول کاغذی و کارت اعتباری و بانک نیست. شما تبدیل به والدی شدین که باید با ارزهای دیجیتال پول تو جیبی فرزندانتون رو در اختیارشون بگذارین. شما کیف پولی مخصوص اعضای خانواده ایجاد می‌کنین و به قابلیتی نیاز دارین که بچه‌ها فقط با تائید والدین بتونن پول برداشت کنن.

قابلیت چند امضایی



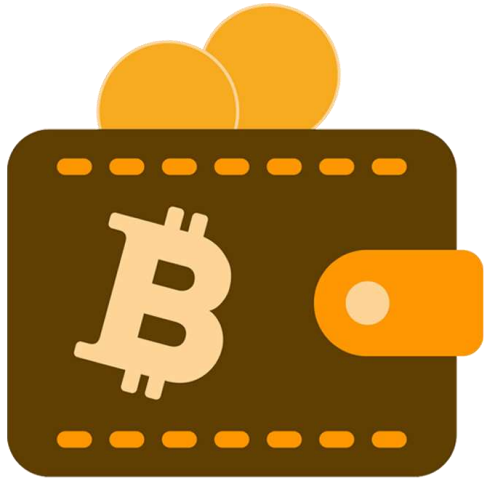
اینجاست که قابلیت Multisig کیف پولهای دیجیتال به کارتون میاد با ایجاد یک کیف پول چند امضایی ، فرزندانتون فقط با تائید و امضای دیجیتال شما قادر به برداشت پول خواهند بود . امروزه تعدادی از کیف پول‌ها مثل کیف پول Bitpay با اضافه کردن قابلیت جدیدی به نام Multisig (چند امضایی یا Multi Signature) ، این امکان رو فراهم کردن که انجام هر تراکنش به امضای بیش از یک نفر نیاز داشته باشه.

آدرس bECH32 یا Segwit یا Default

3 BECH32 یا Segwit یا Default

Bech32 ، جدیدترین و پیشرفته‌ترین آدرس بیت کوین در مقایسه با دو آدرس دیگر هست. این آدرس با کاراکتر bc1 شروع می شه و طولانی‌تر از آدرس‌های P2PKH و P2SH هست. سرعت انجام معاملات با آدرس Bech32 با وجود هزینه کمتر، در مقایسه با دو آدرس دیگه بیشتر هست . همچنین این فرمت با اسم سگویت (Segwit) نیز شناخته میشه.

سازگاری آدرس های بیت کوین با هم



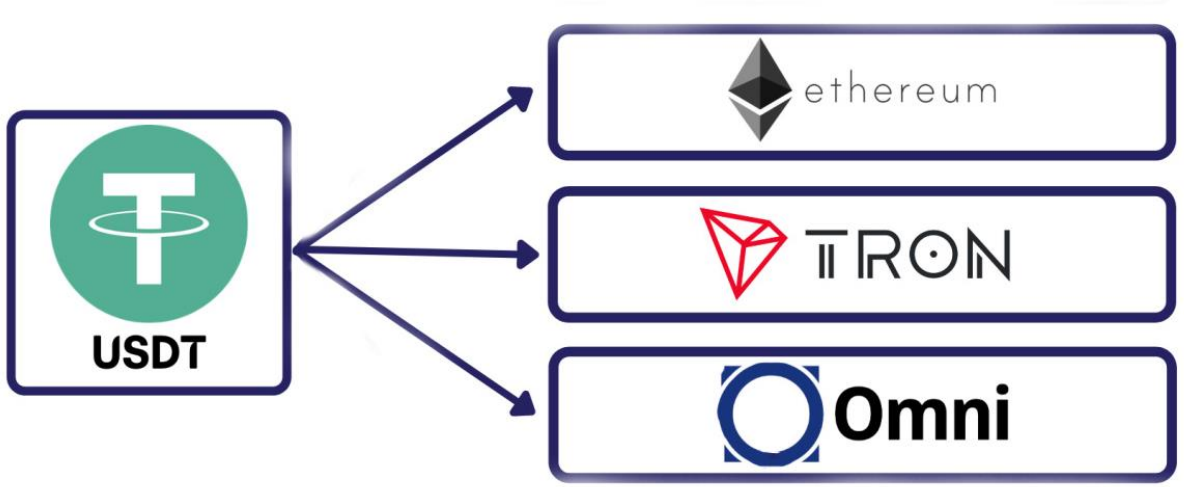
1. P2PKH یا Legacy
2. P2SH یا Compatibility
3. BECH32 یا Segwit یا Default

دقت داشته باشین که در شبکه بیت کوین لزومی بر یکی بودن پیشوند آدرس های کیف پول ها وجود نداره و از هر فرمت آدرسی میشه به آدرس با فرمت دیگه بیت کوین خودتون رو انتقال بدید.

مثال انتقال تتر - مقدمه

شما بعد از خرید استیبل کوین تتر در صرافی (مثلا نوبیتکس) احتمالا بخواین اون رو انتقال بدین ، اینجا گزینه های مختلفی پیش روی شما هست که احتمال داره شمارو گیج کنه و ندونین تتر خودتون رو از چه راهی (روی چه بستری) منتقل کنید .

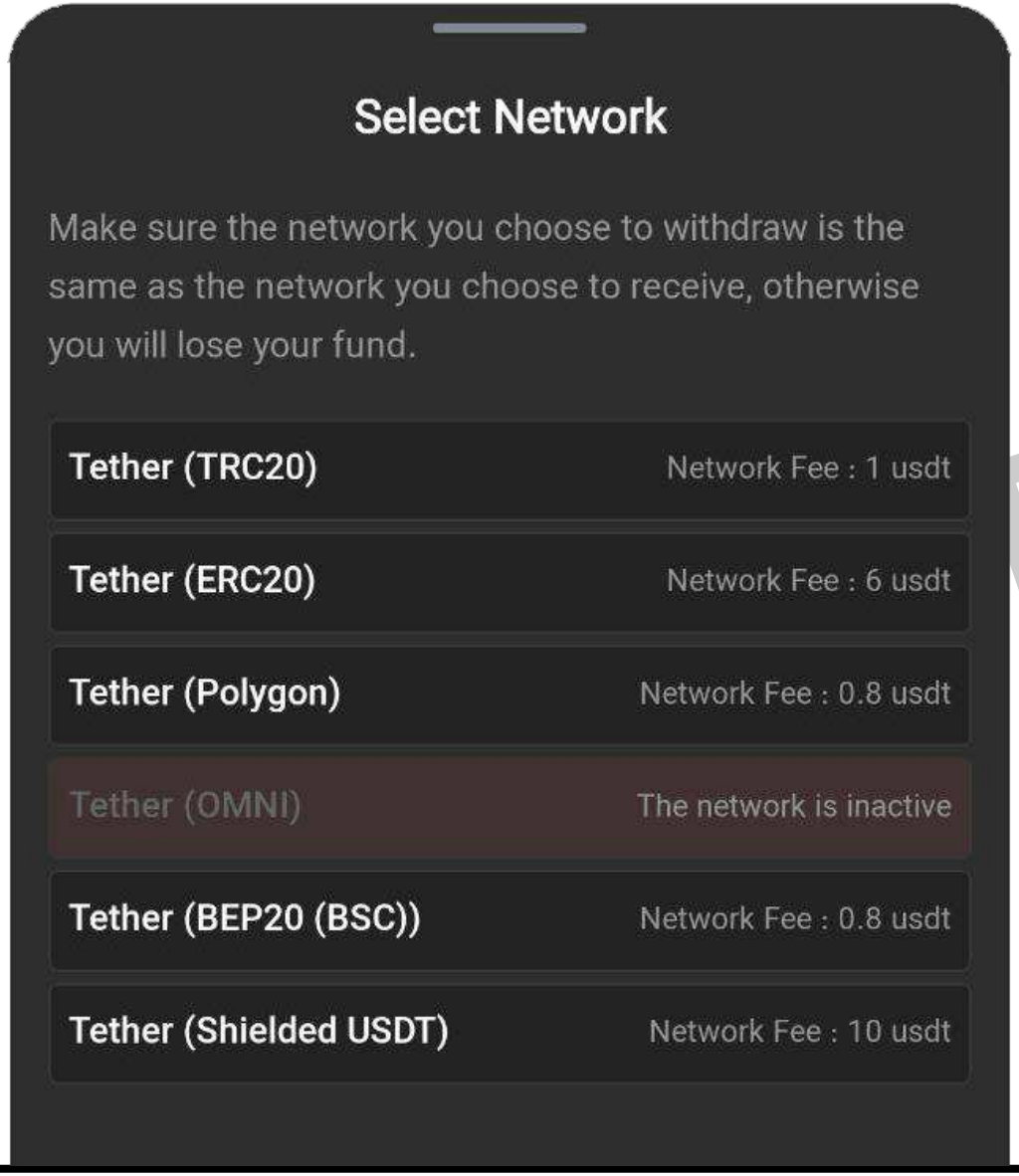
مثال انتقال تتر – انواع شبکه انتقال



- همونطور که میدونید تتر یک توکن هست که از خودش بلاکچین مستقل نداره و باید توسط دیگر بلاکچین ها پشتیبانی بشه .

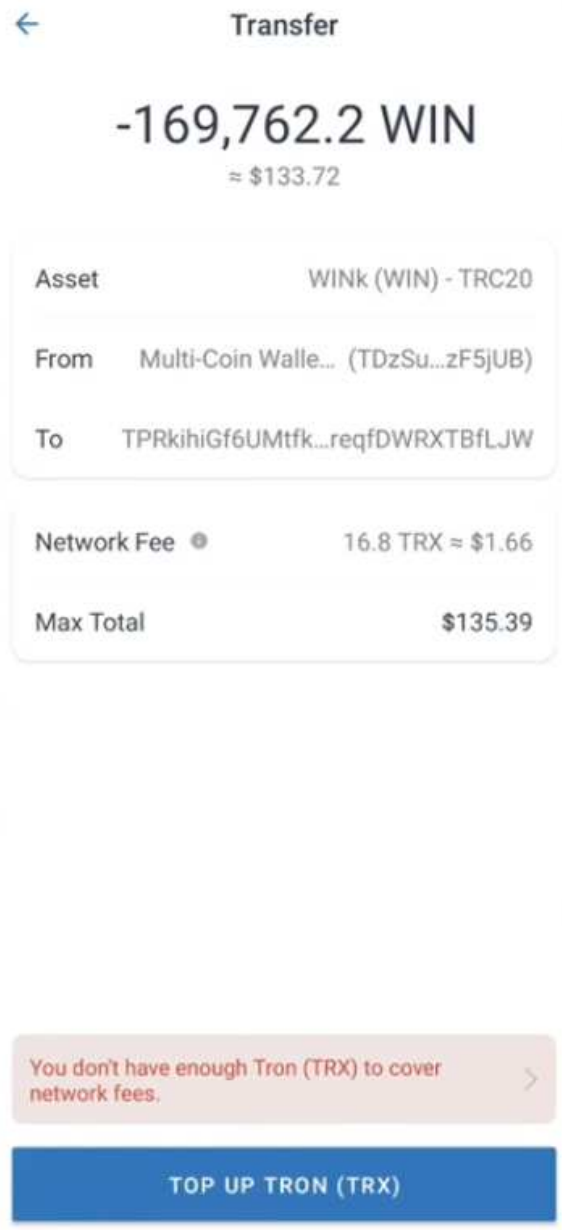
- برای انتقال تتر میتونید از شبکه های مختلفی استفاده کنید که با توجه به پارامتر های انتقال باید تصمیم بگیریم که از چه شبکه ای استفاده کنیم .

مثال انتقال تتر - کارمزد



- اگر پارامتر کارمزد رو لحاظ کنیم در شکل روبرو میتونید کارمزد انتقال تتر رو در شبکه های مختلف ببینید .
- همونطور که میبینید شبکه پالیگان برای انتقال تتر کارمزدپایین تری رو میگیره و خب سرعت خوبی هم داره ، پس شاید انتخاب مناسبی باشه .
- بهتره نسبت به کارمزد ها دید خوبی داشته باشید تا بتونید یک انتقال به صرفه رو انجام بدید ، مثلا برای انتقال تتر کارمزد در حدود ۱ تا ۱۰ دلار ، در شبکه های مختلف هست .

نوع کارمزد



- باید این رو بدونیم که انتقال روی هر شبکه ای انجام بشه ، بعنوان کارمزد باید کوین بومی همون شبکه رو پرداخت بکنیم .

- برای مثال انتقال وینک روی شبکه ترون نیازمند این هست که شما (به اندازه ی کارمزد) در کیف پول خودتون ترون داشته باشید تا شبکه بتونه کارمزد خودش رو برداره . که در این مثال تقریبا ۱۷ ترون هست .

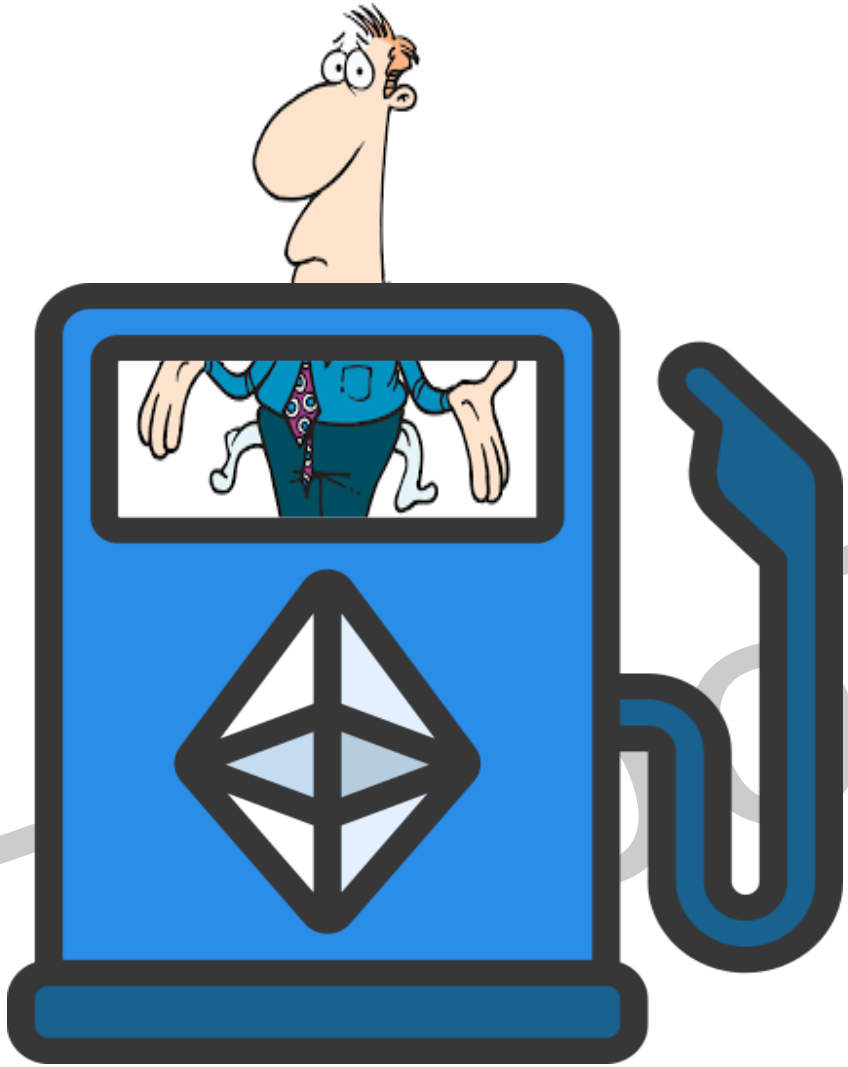
تفاوت کسر کارمزد در انواع کیف پول ها

همونطور که میدونید برای یک انتقال دارایی ، کارمزدی به شبکه داده خواهد شد . اما نحوه پرداخت این کارمزد در انواع کیف پول ها متفاوت هست

- کیف پول های سخت افزاری : از ارز بومی بلاکچین موجود در کیف پول کسر می شه (نه از دارایی انتقال داده شده)
- کیف پول های نرم افزاری : از ارز بومی بلاکچین موجود در کیف پول کسر می شه (نه از دارایی انتقال داده شده)
- کیف پول های آنلاین (کیف پول های صرافی های متمرکز) : از خود دارایی انتقال داده شده کسر میشه .

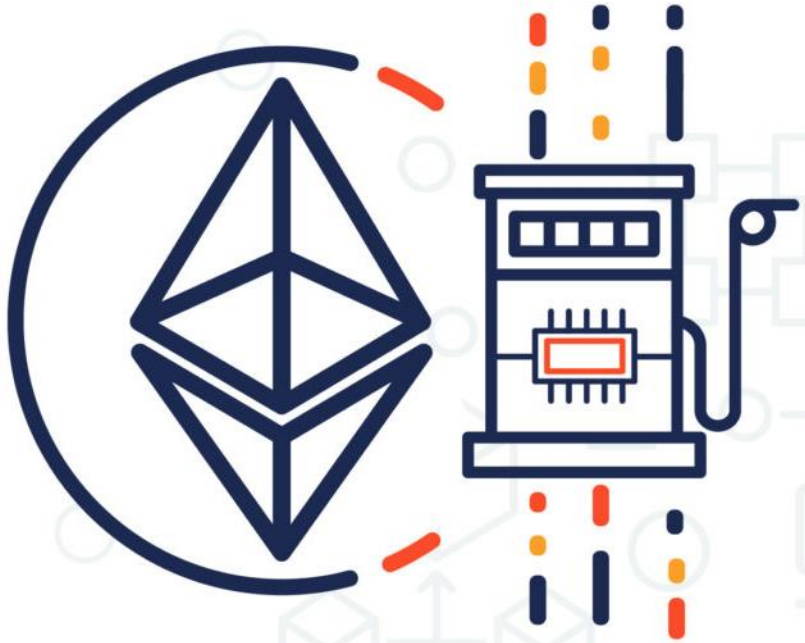
بنابر این در کیف پول های سخت افزاری و نرم افزاری موقع انتقال یک توکن باید ارز بومی بلاکچینی که شبکه انتقال اون رو استفاده میکنید حداقل به اندازه ی کارمزد تراکنش ، در کیف پول خود موجود داشته باشید تا با پرداخت کارمزد از ارز بومی ، انتقال انجام بشه .

توجه به کارمزد و مبلغ انتقالی



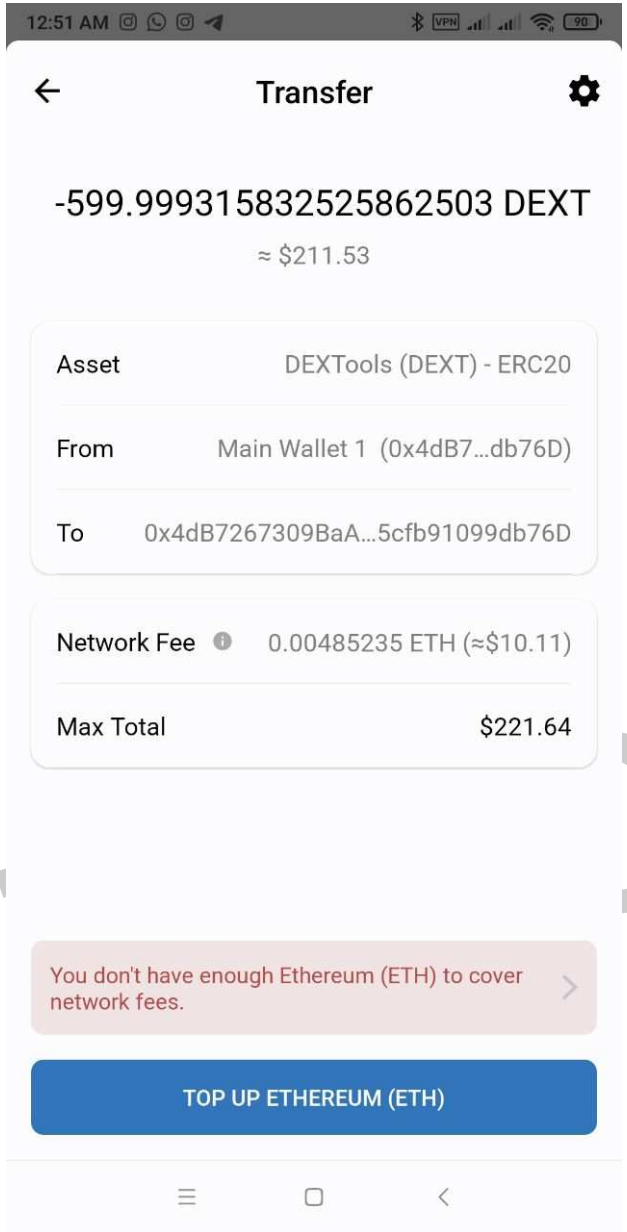
- گفتیم وقتی در حال انتقال یک دارایی هستیم ، کارمزد برامون پارامتر مهمی محسوب میشه ، برای همین باید بتونیم حساب کنیم آیا دارایی من اونقدری هست که به انتقالش ارزش داشته باشه ؟
- مثلا کسی که در نوبیتکس ۳ تتر داره آیا میرزه برای انتقالش به تراست ولت ۱ تتر پرداخت بکنه ؟

انتقال با سرعت پایین ولی کارمزد کمتر



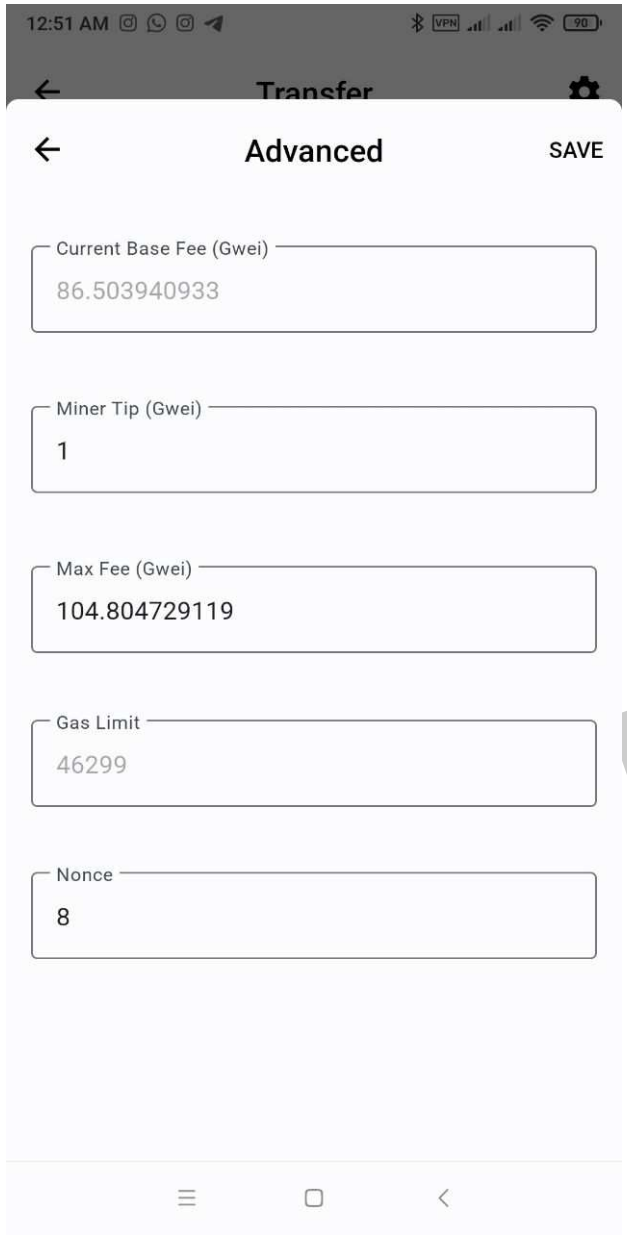
در ابتدای بحث که به پارامتر های انتقال اشاره کردیم ، توضیح دادیم که انتخاب پارامتر های انتقال ، بستگی به شرایط شما داره . در مبحث انتقال مدلی وجود داره که میتونید در ازای انتقال دیر تر ، کارمزد کمتری رو پرداخت بکنید . البته این موضوع در مورد همه ی دارایی ها امکان پذیر نیست .

مثال انتقال با سرعت پایین ولی کارمزد کمتر



در مثال روبرو قصد انتقال مقداری DEXT رو داریم که باتوجه به مقدار فی شبکه باید 10.11 دلار کارمزد (معادل دلاری اتریوم لحاظ شده) پرداخت کنیم .

مثال انتقال با سرعت پایین ولی کارمزد کمتر

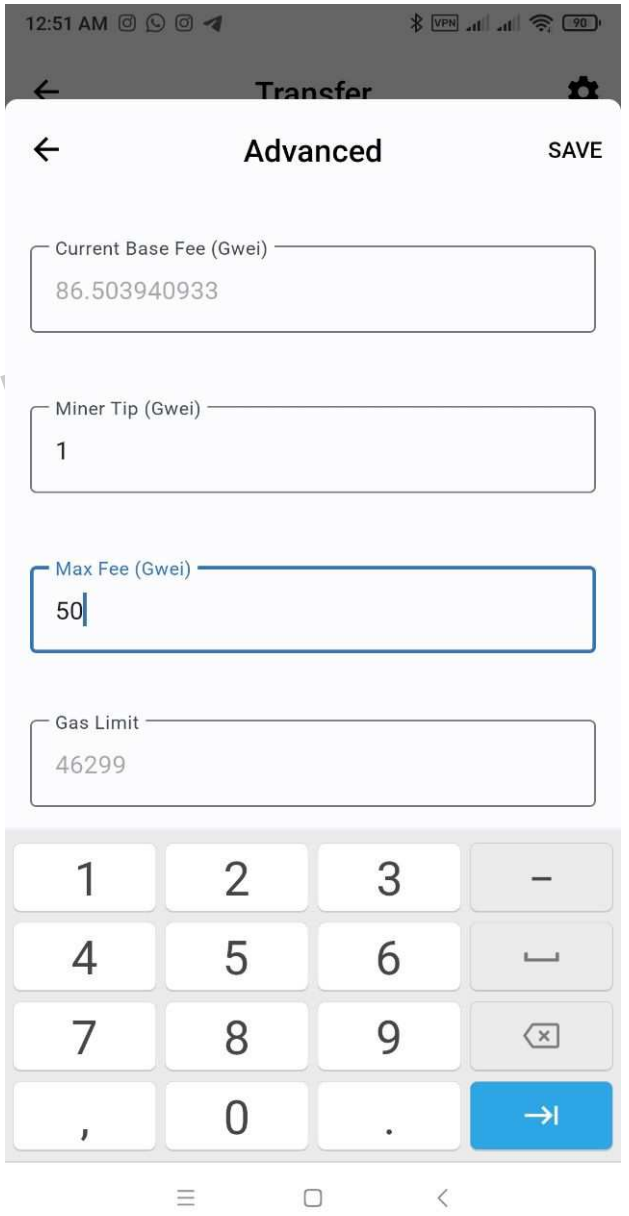


با مراجعه به تنظیمات

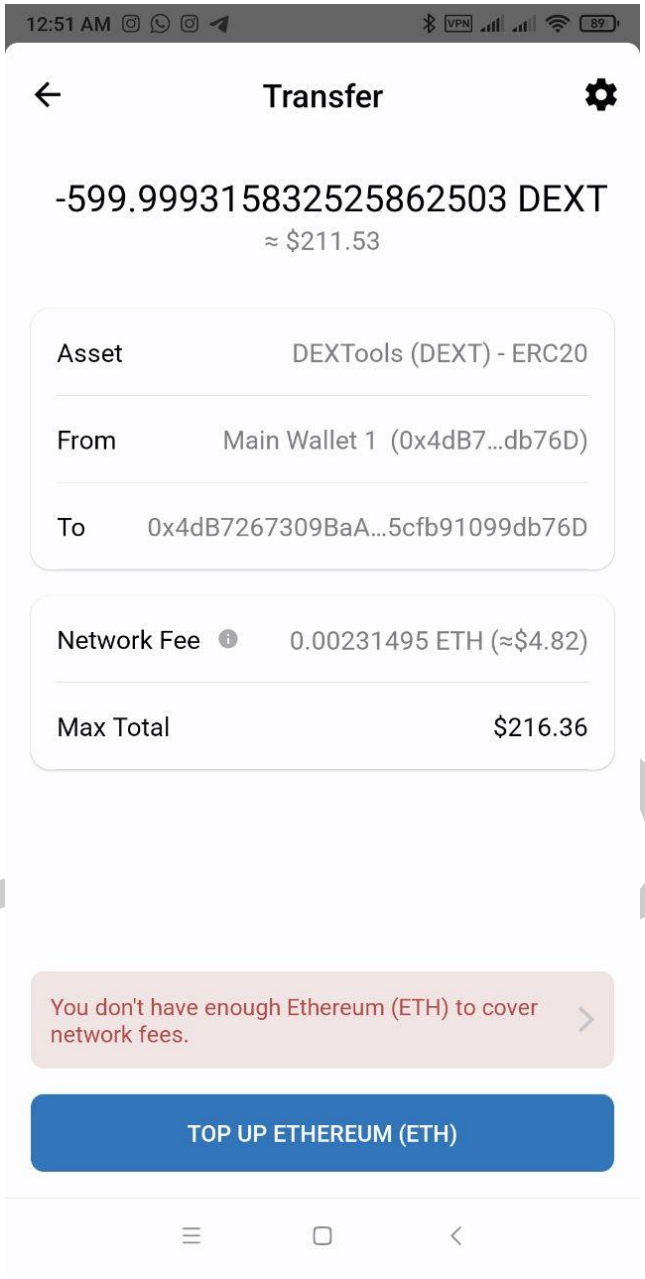
مقدار Max Fee رو

از ۱۰۴ به ۵۰

کاهش میدیم



مثال انتقال با سرعت پایین ولی کارمزد کمتر

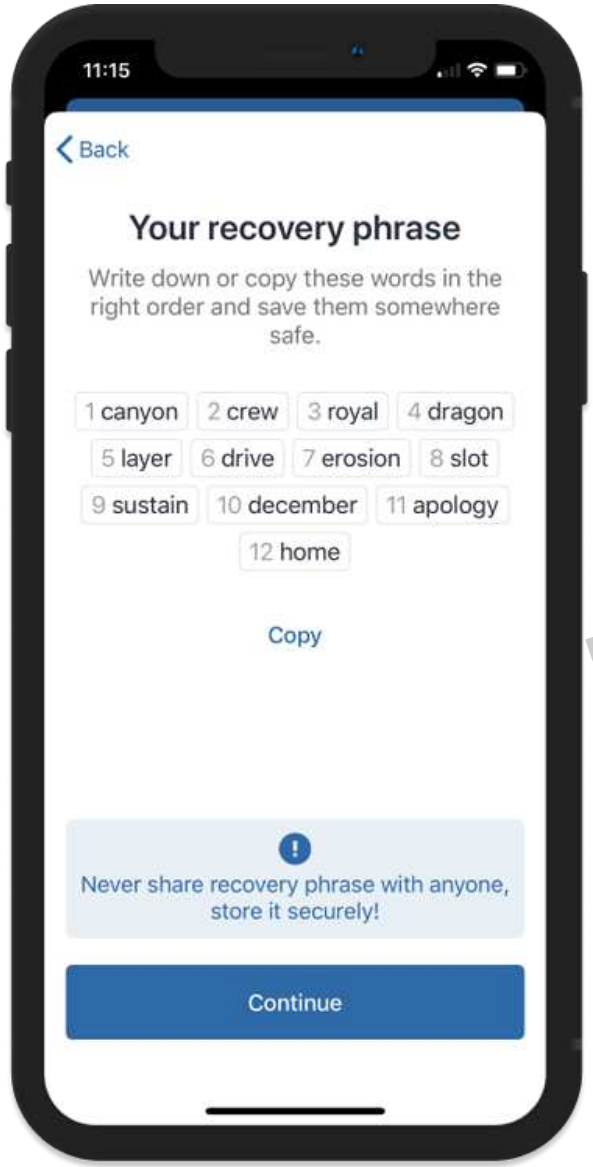


همونطور که میبینید با کم کردن این مقدار ، میزان کارمزد از 10.11 دلار به 4.82 دلار کاهش یافت ، اما زمان انتقال رو افزایش دادیم .

وارد کردن Seed Phrase در ولت دیگر

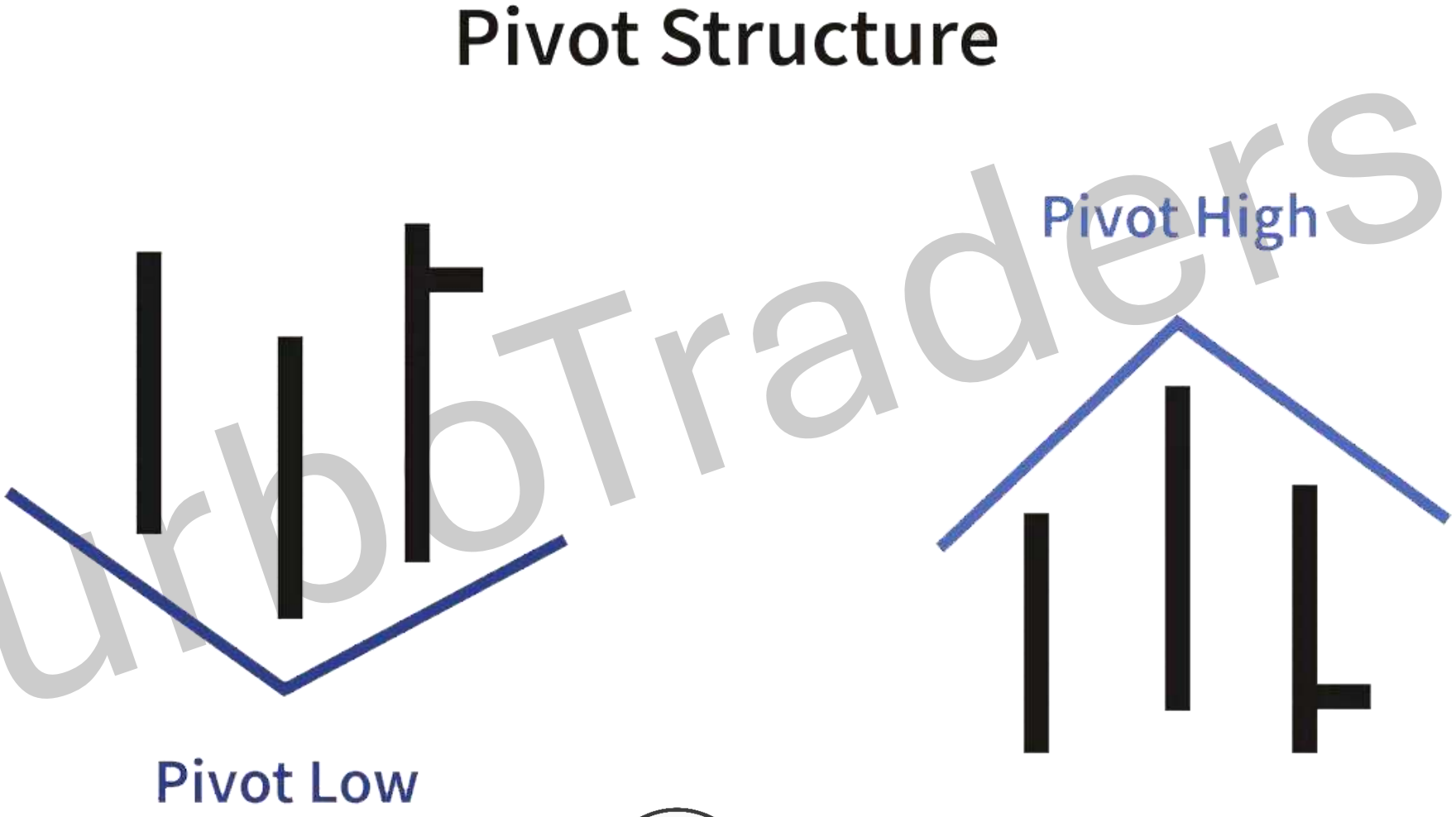
عبارات بازیابی یا Seed Phrase بر اساس طرح BIP39 میتونه از ۱۲، ۱۵، ۱۸، ۲۱ یا ۲۴ کلمه تشکیل بشه . باید بدونیم که اگر در یک ولت (مثلا تراست ولت) دارایی داشتیم ، میتونیم اون رو در ولت دیگری باز کنیم ، البته به شرط اینکه عبارت بازیابی خودمون رو فراموش نکرده باشیم .

هرگز نباید عبارات بازیابی کیف پول خودتون رو گم کنید !



همونطور که میدونین بر خلاف کیف پول های آنلاین (مثل کیف پول های صرافی های متمرکز) در کیف پول های نرم افزاری ، سخت افزاری و کاغذی کلید خصوصی تنها دست شماست و یا روی دستگاه خودتون ذخیره میشه . بنابراین گم کردن عبارت بازیابی به معنی عدم دسترسی شما به کلید خصوصی شماست و نداشتن کلید خصوصی به معنی عدم دسترسی به داراییتون خواهد بود و به دلیل غیر متمرکز بودن سیستم بلاکچین ، کلید خصوصی شما روی هیچ سروری ذخیره نشده و هیچ ارگان یا سازمانی امکان بازگرداندن دارایی شما رو نداره چون جز شما هیچ کس کلید خصوصی کیف پول شما رو نداشته و نخواهد داشت . پس در نگهداری ۱۲ کلمه عبارت بازیابی خودتون بسیار حساس باشید.

Major and minor



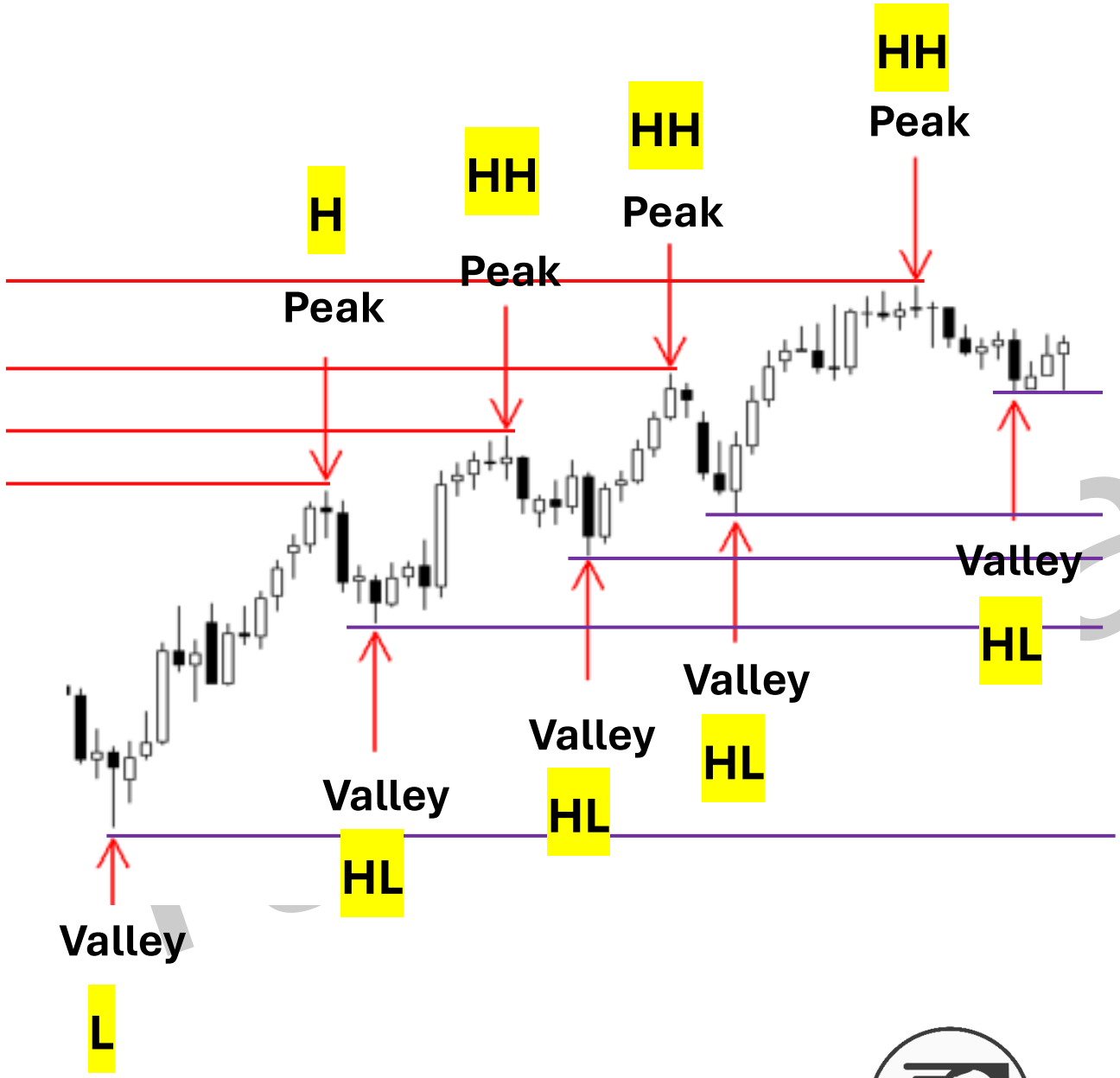
تنظیم مقیاس نمودار

تنظیم نادرست مقیاس

تنظیم نادرست مقیاس

Trends Types

سقف و کف قیمت



- سقف و کف قیمت رو میتونیم مثل قله و دره در نظر بگیریم . در مارکت به این قله و دره ها ، سقف قیمتی و کف قیمتی در یک بازه گفته میشه .
- تعریف :

  سقف قیمتی : High یا به اختصار H

  کف قیمتی : Low یا به اختصار L

- چهار حالت ممکنه با توجه به تعریف :

  HH و HL و LL و LH


مثال
Ethereum / TetherUS · 4h · BI NCE
O1843.72 H1848.79 L1834.23 C1839.00 −4.73 (−0.26%)
ETHUSDT
USDT
1838.99
0.01
1839.00
H
LH
L
LH
LL
LH
LL
LH
HH
HL
LL
1720.00
1680.00
1640.00
1600.00
1560.00
1520.00
1480.00
1440.00
1400.00
1360.00
1315.48
1280.00
1240.00
1200.00
TradingView
8
12
15
19
22
26
15:30
Oct
4
7
1D
5D
1M
3M
6M
YTD
1Y
5Y
All
11:25:58 (UTC+3:30)
%
log
auto


مثال
1D · CRYPTO
O22823.21 H23285.02 L22339.66 C23139.10 +314.97 (+1.38%)
L
H
HL
HH
HL
HH
LL
LH
LL
LH
70000.00
62500.00
60000.00
57500.00
55000.00
52500.00
50000.00
47500.00
45000.00
42500.00
40000.00
37500.00
35041.11
32500.00
30000.00
27500.00
25000.00
22500.00
20000.00
17500.00
15000.00
12500.00
10000.00
7500.00
11
20
Feb
15
Mar
15
Apr
12
21
May
10
19
Jun
14
1Y
5Y
All
20:07:01 (UTC+3:30)


Euro / U.S. Dollar · 4h · FXCM
O1.08847 H1.09087 L1.08814 C1.08998 +0.00151 (+0.14%)
1.08998
0.2
1.09000
H
LH
L
LH
LL
LH
LL
LH
LL
LL
1.11200
1.11000
1.10800
1.10600
1.10400
1.10200
1.10000
1.09800
1.09600
1.09400
1.09200
1.08998
1.08918
1.08800
1.08600
1.08400
1.08200
1.08000
1.07800
1.07600
1.07400
1.07200
1.07000
1.06800
1.06600
1.06400
1.06200
TradingView
8
10
15
17
22
24
29
Jun
5
7
12
14
19
21
26
1D 5D 1M 3M 6M YTD 1Y 5Y All
19:55:53 (UTC+3:30)


Bitcoin / U.S. Dollar · 1D · CRYPTO
O22823.21 H23285.02 L22339.66 C23139.10 +314.97 (+1.38%)
66466.22
0.00
66466.22
L
H
HL
HH
HL
HH
LL
LH
LL
LH
TradingView
Fri 18 Dec '20
2021
11
20
Feb
15
Mar
15
Apr
12
21
May
10
19
Jun
14
1D 5D 1M 3M 6M YTD 1Y 5Y All
20:07:01 (UTC+3:30)

SaeedGL1 published on TradingView.com, Mar 06, 2024 20:12 UTC+3:30

TradingView