

پلاریوم سامانه مدیریت کلید Crypto KMS

تهیهکننده: استارتاپ پلاریوم

نسخه مستند: ۱/۱

تاریخ مستند: ۱۴۰۲/۰۹/۰۸

تاریخچه نگارش

تاريخ ويرايش	تغييرات ويرايش	ويرايش
1604/09/01	ایجاد سند	1/0
1404/09/04	بروزرسانی سرویسها	1/1

فهرست مطالب

مه	۱ - مقد
اف مستندا	۲ - اهد
رد کلی	
١X-Apı-	
سب کلید	
ن استخراج کلید	
رویسهای مدیریت کلید	س – ۴
ت کلید جدید	ساخ
دن کلید براساس کلید خصوصی	افزود
دن کلید براساس MNEMONICS.	افزود
٠ کليد	
اق کلید	
غراج کلید	
رویسهای شبکههای مبتنی بر اتریوم	۵ – س
ا توسط کلید	امضا
فت اطلاعات عمومی کلید	درياذ
رویسهای شبکههای مبتنی بر UTXO	۶ – سر
ا توسط کلید۸	امضا
فت اطلاعات عمومي، كليد	د، ياف



۱ - مقدمه

مجموعـه ســرویسهای Blockchain as a Service پلاریــوم تــلاش مــیکنــد تــا زمــان توســعه محصــول را بــرای مشــتریان خــود در حــوزه بلاکچــین را کــاهش داده و نیــاز و وابسـتگی آنهـا را بـه دانـش فنـی مـرتبط بـا بلاکچـین بـه حـداقل میــزان ممکـن برسـاند. بـدین ترتیــب کســبوکارهای نوپـا و نیــز ســازمان یافتــه مــیتواننــد در ســریعترین زمــان ممکـن بــا اسـتفاده از ســرویسهـای مبتنــی بــر وب پلاریــوم محصـولات خـود را توسـعه و گسترش دهند.

۲ - اهداف مستند

ایـن مسـتند در راسـتای معرفی سـرویسهای مـدیریت کلیـد مبتنـی بـر بلاکچـین (Crypto) میباشــد. بــر اســاس طراحــی ســامانههای پلاریــوم، (Key Management Service پلاریــوم میتواننــد کلیــدهای خـود را در بـیش از یـک محــل ذخیــره کنند.

در ایــن راســتا، ســرویسهای KMS بــه صــورت مســتقل از Wallet ارائــه شــده اســت و قابلیـت ایـن را دارد کـه بـه صـورت اختصاصـی بـرای مشـتریان نصـب شـده و یــا اینکـه بـه صورت مشترک و از سرویس مدیریت کلید cloud پلاریوم استفاده نماید.

۳ - موارد کلی

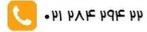
X-Api-Key •

مقدار api-key یک رشته تولید است که جهت احراز هویت و تنظیم دسترسی به سرویسها استفاده می شود.

• برچسب کلید

در بعضی از عملیات کاربر میتواند یک برچسب (Label) برای خود مشخص کند. در آینده این برچسب جهت تحلیل دادهها توسط کاربر در داشبورد میتواند مورد استفاده قرار گیرد.







• امكان استخراج كليد

در هنگام ثبت اطلاعـات کلیـد و یـا تولیـد کلیـد در سـامانه، کـاربر میتوانـد بـا مقـدار دهـی بـه فیلـد Exportable=true مشـخص کنـد کـه در آینـده امکـان اسـتخراج اطلاعـات کلیـد وجـود خواهد داشت.

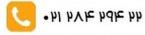
۴ - سرویسهای مدیریت کلید

• ساخت کلید جدید

این سرویس یک کلید کاملاً جدید تولید می کند و شناسه یکتای آن را باز میگرداند.

Generate Key				
<server-url>/api/ke</server-url>	<server-url>/api/keys/generate</server-url>			
	Method	POST		
	Header	Content-Type	application/json	
Request	rieauei	X-API-Key	Authorization Token	
	Body	<pre>{ "label": "< "exportable" }</pre>	string>", ': " <boolean>"</boolean>	
Dagagag	keyld			شناسه یکتای کلید
Response	Example	{ "keyId": " <u td="" }<=""><td>uuid>"</td><td></td></u>	uuid>"	







• افزودن کلید براساس کلید خصوصی

این سرویس یک کلید را بر اساس کلید خصوصی در سیستم ثبت میکند.

لازم به ذکر است که مقدار chaincodeHex یک مقدار اختیاری است و جهت اشتقاق کلید است و جهت اشتقاق کلید است که نیازی به آن ندارید کلید استفاده میگردد و در صورتی که نیازی به آن ندارید می توانید مقدار آن را null ارسال کنید. جهت دریافت اطلاعات بیشتر لطفاً به مستندات BEP-۰۰۳۲۴ مراجعه بفرمایید.

Import-Privatekey			
<server-url< td=""><td>>/api/keys/import-privatekey</td><td></td><td></td></server-url<>	>/api/keys/import-privatekey		
	Method	POST	
	Header	Content-Type	application/json
Request	rieddel	X-API-Key	Authorization Token
	Body	"chainCodeHe": "<	dex": " <string>", ex": "<string>", string>", ': "<boolean>"</boolean></string></string>
Respons	keyld		کلید یکتا
е	Example	{ "keyId": "< }	uuid>"

• افزودن کلید براساس Mnemonics

ایـن سـرویس یـک کلیـد خصوصـی بـر اسـاس mnemonic ارسـال شـده در سـامانه ثبـت میکند.

^۲ https://github.com/bitcoin/bips/blob/master/bip-۰۰٣٢.mediawiki







¹ Key Deriviation



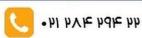
Import-Privatekey			
<server-url>/api/keys/import-mnemonics</server-url>			
	Method	POST	
	Header Request	Content-Type	application/json
Request		X-API-Key	Authorization Token
	Body	"label": "<	: " <string>", string>", ': "<boolean>"</boolean></string>
Dognanaa	keyld		کلید یکتا
Response	Example	{ "keyId": " <u td="" }<=""><td>uuid>"</td></u>	uuid>"

• حذف كليد

با ایـن سـرویس کـاربر میتوانـد بـا ارائـه شناسـه کلیـد (تولیـد شـده در سـرویسهای فـوق) اقـدام بـه حـذف کلیـدی کـه از آن کلیـد دیگـری مشـتق شـده باشـد، مشـکلی بـه وجـود نخواهـد آمـد و در واقـع تنهـا کـاربر اسـت کـه ارتبـاط بـین کلیدها را میداند.

Delete Key			
<server-url>/a</server-url>	api/keys/delete		
	Method	POST	
Doguest	Request Header	Content-Type	application/json
Request Header	ricauci	X-API-Key	Authorization Token
	Body	{ "keyId": " }</td <td>string>",</td>	string>",
Response	keyld		کلید یکتا
Example		frayvy-ersr-rac	cY-a•Fd-ceY&A9YFdb&V•Y







• اشتقاق کلید

ایــن ســرویس امکــان انشــقاق کلیــد (Key Deriviation) بــر اســاس اســتاندارد BEP-۰۰۳۲ را بــه کــاربر میدهــد. لازم بــه ذکــر اســت کــه کلیــد جدیــد تولیــد شــده نیــز امکــان اشــتقاق را خواهد داشت.

Derive Key				
<server-url></server-url>	<server-url>/api/keys/derive</server-url>			
	Method	POST		
	Header	Content-Type	application/json	
Request		X-API-Key	Authorization Token	
	Body	<pre>{ "parentId": "<uuid>", "label": "<string>", "exportable": "<boolean>" }</boolean></string></uuid></pre>		
Dooponoo	keyld		کلید یکتا	
Response	Example	{ "keyId": " <br }	uuid>"	

• استخراج کلید

با کمک ایان سرویس میتوانید مقدار کلید خصوصی، chain code و سایر اطلاعات کلید را دریافت نمایید. در صورتی که در زمان تولید کلید، آن را exportable معرفی نکرده باشید، امکان export آن وجود نخواهد داشت.







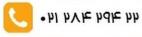
Export Key				
<server-url>/ap</server-url>	<server-url>/api/keys/export-key</server-url>			
	Method	GET		
Request	Header	Content-Type	application/json	
Request	Tieauei	X-API-Key	Authorization Token	
	Query Params	"keyId": " <uuid>"</uuid>		
	privatekeyHex	لید خصوصی در مبنای شانزده		
	chainCodeHex	مخصوص به صورت hex		
	timestamp	مان دریافت کلید		
Response	label	مان دریافت کلید رچسب کلید		
Example		"timestamp"	Hex": " <string>", : "<datetime>", ex": "<string>", string>"</string></datetime></string>	

۵ - سرویسهای شبکههای مبتنی بر اتریوم

• امضا توسط كليد

این سرویس hash یک تراکنش را بر اساس کلید مشخص شده امضا میکند.





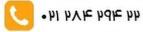


Signs Transaction Hash				
<server-url>/api/evm/sign/hash</server-url>				
	Method	POST		
	Header	Content-Type	application/json	
Request	Tieauei	X-API-Key	Authorization Token	
	Body	<pre>{ "keyId": "< "hashHex": ' "chainId": ' }</pre>	" <string>",</string>	
	keyld			کلید یکتا
	hashHex			مقدار هش به صورت hex
Response	chainId			کد یکتای شبکه
	Example	<pre>{ "r_Hex": "<string>", "s_Hex": "<string>", "v_Hex": "<string>", "signature": "<string>" }</string></string></string></string></pre>		

• دریافت اطلاعات عمومی کلید

ایــن ســرویس اطلاعــات کلیــد و آدرس تولیــد شــده بــر اســاس اســتانداردهای شــبکههای مبتنی بر اتریوم را مشخص میکند.







Returns public information			
<server-url>/api/evm/get-public-info</server-url>			
	Method	GET	
Request	Header	Content-Type	application/json
	neauei	X-API-Key	Authorization Token
	keyld		کد یکتای کلید
	publicKeyHex		کلید عمومی
Response	publicAddress	آدرس اتریمی	
	Example		uuid>", ex": " <string>", ess": "<string>"</string></string>

۶ - سرویسهای شبکههای مبتنی بر UTXO

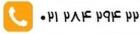
در ایـن بخـش سـرویسهای شـبکه هـای مبتنـی بـر سـاختار UTXO " ماننـد بیـت کـوین توضیح داده خواهند شد.

• امضا توسط كليد

ایـــن ســرویس یــک تــراکنش را رمــز میکنــد. لازم بــه ذکــر اســت کــه مقــدار hexadecimal در واقــع داده json تــراکنش اســت کــه بــه صــورت transactionDataHex کـد شـده اسـت. ایـن سـرویس تـلاش میکنـد کـه ورودیهـای تـراکنش را توسـط کلیـدهای ارائـه شـده امضـا نمایـد. بـدیهی اسـت کـه در صـورت عـدم ارائـه تمـامی کلیـدها، تـراکنش تولید شده در خروجی، به طور کامل رمز نشده باشد.

ایـن موضـوع بـه کـاربر امکـان ارائـه سـرویس رمزنگـاری یـک تـراکنش توسـط چنـدین نفـر را میدهد به این صـورت کـه هـر یـک از کـاربران اطلاعـات تـراکنش را بـه صـورت جداگانـه رمـز میکند و نتیجه را در اختیار نفر بعد قرار میدهد.





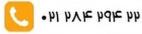


Signs a UXTO (like bitcoin) transaction				
<server-url> /api/utxo/sign-tx</server-url>				
	Method	POST		
	Header	Content-Type	application/json	
Request	Headel	X-API-Key	Authorization Token	
, request	Body	<pre>{ "keyIds": ["<uuid>", "<uuid>"], "transactionDataHex": "<string>", "network": "MainNet" }</string></uuid></uuid></pre>		
Response	Hash string	داده تراکنش UTXO که به صورت hex کد شده است.		
	Example	<string></string>		

• دریافت اطلاعات عمومی کلید

ایــن ســرویس اطلاعــات کلیــد و آدرس تولیــد شــده بــر اســاس اســتانداردهای شــبکههای مبتنی بـر UTXO ماننـد بیتکـوین را مشـخص میکنـد. بـا توجـه بـه اینکـه آدرس تولیــد شــده ممکـن اســت کـه بــر اســاس نــوع شــبکه (mainnet و یــا testnet و ...) متفــاوت باشــد، کــاربر میبایست نوع شبکه خود را مشخص نماید.







Returns public information (public key and address based on utxo networks)

<server-url> /api/utxo/get-public-info

	Method	GET		
Request	Header	Content-Type	application/json	
	ricadei	X-API-Key	Authorization Token	
	Query	Keyld	کد یکتای کلید	
	Query	ChainType	نوع شبکه	
	keyld		کد یکتای کلید	
	publicKeyHex		کلید عمومی	
Response	nse publicAddress		آدرس در شبکه	
Example		<pre>{ "keyId": "<uuid>", "publicKeyHex": "<string>", "publicAddress": "<string>" }</string></string></uuid></pre>		



