



منتشر شده توسط

نویسنده: مینو علی خانی

کوین ایران



ایمیل نویسنده: alikhaniminoo@yahoo.com

کوین ایران بزرگترین پایگاه خبری فارسی زبان در حوزه فناوری بلاکچین، ارزهای رمزنگاری شده و پلتفرم های مرتبط با بلاکچین است. این وب سایت در سال ۱۳۹۲ توسط بابک جلیوند و آرش محبوب، با هدف اطلاع رسانی، آموزش و مشاوره به جامعه فارسی زبان علاقه مند به رمز ارزها راه اندازی شد و اولین مقاله آن در ۱۴ دی ماه همان سال، با عنوان «بیت کوین چیست؟» منتشر گردید. هدف کوین ایران از معرفی این فناوری ایجاد محیطی پژوهشی و آموزشی در راستای استفاده صحیح از این فناوری جهت ارائه تسهیلات و رفاه به جوامع فارسی زبان است.

www.coiniran.com



Zcash چیست و تفاوت آن با سایر ارز های رمزنگاری شده چه می باشد؟

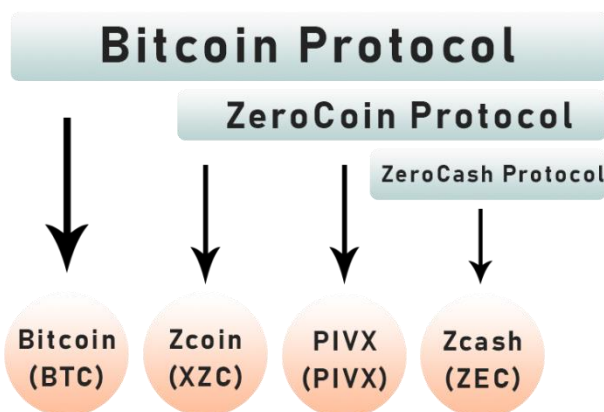
زی کش (Zcash) رمز ارزی است که با هدف ایجاد محیطی امن برای کاربرانی که از همگانی بودن تراکنش رمز ارز هایی چون بیت کوین ناخشنود هستند و می خواهند در اینترنت، تراکنش های گمنام و ناشناس داشته باشند، ساخته شده است. در واقع سازندگان Zcash بر این باورند که در این شبکه، قدرت نهایی در انحصار سازندگان نبوده بلکه در دست کاربران است. با وجود تمرکز زدایی (Decentralization) در شبکه زی کش، امنیت و عدالتی که لازمه هر قرارداد کاری است، برقرار خواهد شد. در ادامه به تاریخچه شکل گیری این رمز ارز می پردازیم.



[Source](#)

تاریخچه:

زی کش در سال 2013 تحت عنوان پروژه ای با نام [Zerocoin](#) با هدف پرداختن به مشکل فقدان حریم خصوصی در تراکنش های بیت کوینی شکل گرفت. پروتکل زی کش، از تغییر و ارتقای پروتکل Zerocoin به سیستم Zerocash و در نهایت تبدیل این سیستم در 28 اکتبر 2016 به پروتکل زی کش، به وجود آمده است. این توسعه و تغییرات توسط شرکت Zerocoin Electric Coin صورت گرفته است که بسیاری از فعالین این حوزه به اشتباه آن را به کمپانی Zcash نسبت می دهند.



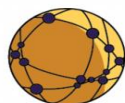
[Source](#)

و اما زی کش چیست؟

زی کش رمز ارزی خصوصی، غیر متمرکز و منبع باز است که از تراکنش های شفاف و محافظت شده پشتیبانی می کند. با آن که پرداخت های زی کش بر روی بلاکچینی عمومی منتشر می شود، اما فرستنده، گیرنده، و تحت شرایطی، میزان تراکنش ها به صورت خصوصی باقی خواهند ماند.

زی کش بر پایه پژوهشی در زمینه ارزیابی دقیق رمزنگاری و توسط تیم مهندسی متخصص در زمینه امنیت پلت فرم با منبع باز ساخته شده است. می توان گفت زی کش حاصل تغییری است که این تیم در زمینه حریم خصوصی بیت کوبین به وجود آورد.

WHAT IS ZCASH?



A decentralized and open-source
cryptocurrency



Shielded transactions hide the
sender, recipient, and value on the
blockchain

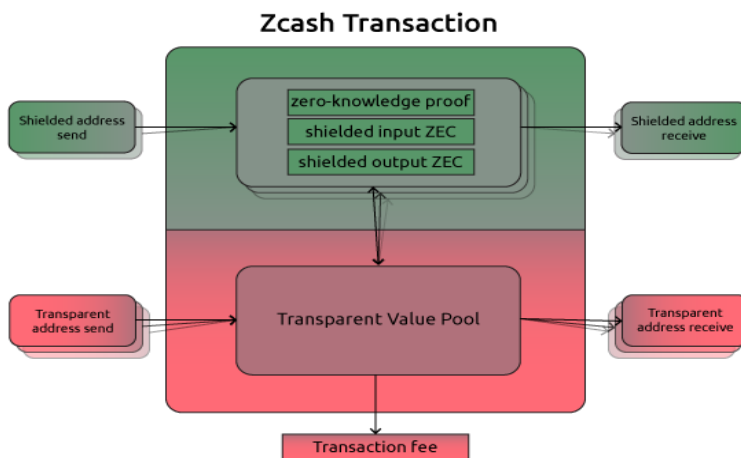


If Bitcoin is like http for money,
Zcash is https—a secure transport
layer

طرز کار زی کش:

زی کش در ابتدا محتوای تراکنش های محافظت شده را رمزنگاری می کند. از آن جایی که اطلاعات پرداختی رمزنگاری شده اند، پروتکل زی کش برای تایید صحت اعتبار آن ها از یک روش تازه رمزنگاری استفاده می کند.

زی کش در واقع از ساخت گواه دانایی صفر [zero-knowledge](#) به نام **zk-SNARK** استفاده می کند که حاصل [پیشرفت های جدید](#) علم رمزنگاری است. چنین ساخت هایی به شبکه زی کش این امکان را می دهند که طرف اثبات کننده صحت گزاره را به طرف دیگر ثابت کند، بدون آن که اطلاعاتی درباره آن گزاره به آن طرف بدهد. به این ترتیب، اطلاعات تراکنش مخفی باقی خواهند ماند.



[Source](#)

زی کش هم چنین این فرصت را در اختیار کاربران قرار می دهد تا پرداخت های عمومی را که مشابه بیت کوین کار می کنند، ارسال کنند. با وجود پشتیبانی از آدرس های محافظت شده و شفاف، انتخاب این که Zcash به صورت محرمانه یا عمومی ارسال شود، بر عهده کاربران است.

پرداخت های زی کش که از آدرس محافظت شده به آدرس شفاف فرستاده می شود، موجودی دریافتی را نشان می دهند؛ این در حالی است که پرداخت های ارسالی از آدرس شفاف به آدرس محافظت شده، از افشای ارزش دریافتی خودداری کرده و آن را نشان نمی دهند.



مقایسه زی کش با بیت کوین:

بارز ترین تفاوت این دو رمزارز، امکان ایجاد تراکنش های ناشناس برای زی کش است؛ در صورتی که با دانستن آدرس والت بیت کوین افراد، قادر خواهید بود که تراکنش های آن حساب را ردیابی کرده و میزان دریافتی و ارسالی حساب او را متوجه شوید.

هم چنین می توان گفت زی کش انشعابی از پروتکل بیت کوین که خود اولین رمزارز بر پایه بلاکچین و دارای استفاده گسترده میان جامعه رمزارزی است، می باشد. با این وجود، زی کش از بلاکچین و توکن رمزارزی خاص خود پشتیبانی خواهد کرد.

زی کش بر روی نمونه هسته فعلی بیت کوین ساخته شده است تا با استفاده از گواه های [zero-knowledge](#) از داده های تراکنش ها محافظت کند.

علی رغم پروژه بیت کوین، زی کش توسط یک شرکت و نه توسط یک جامعه متن باز راه اندازی شده است. به همین دلیل تیم زی کش مجبور به پرداخت هزینه پرسنل شرکت و سود سرمایه گذاران با مالیاتی که روی پاداش های استخراج گذاشته می شود، بوده و اسم این پاداش ها را Founders reward گذاشته اند.

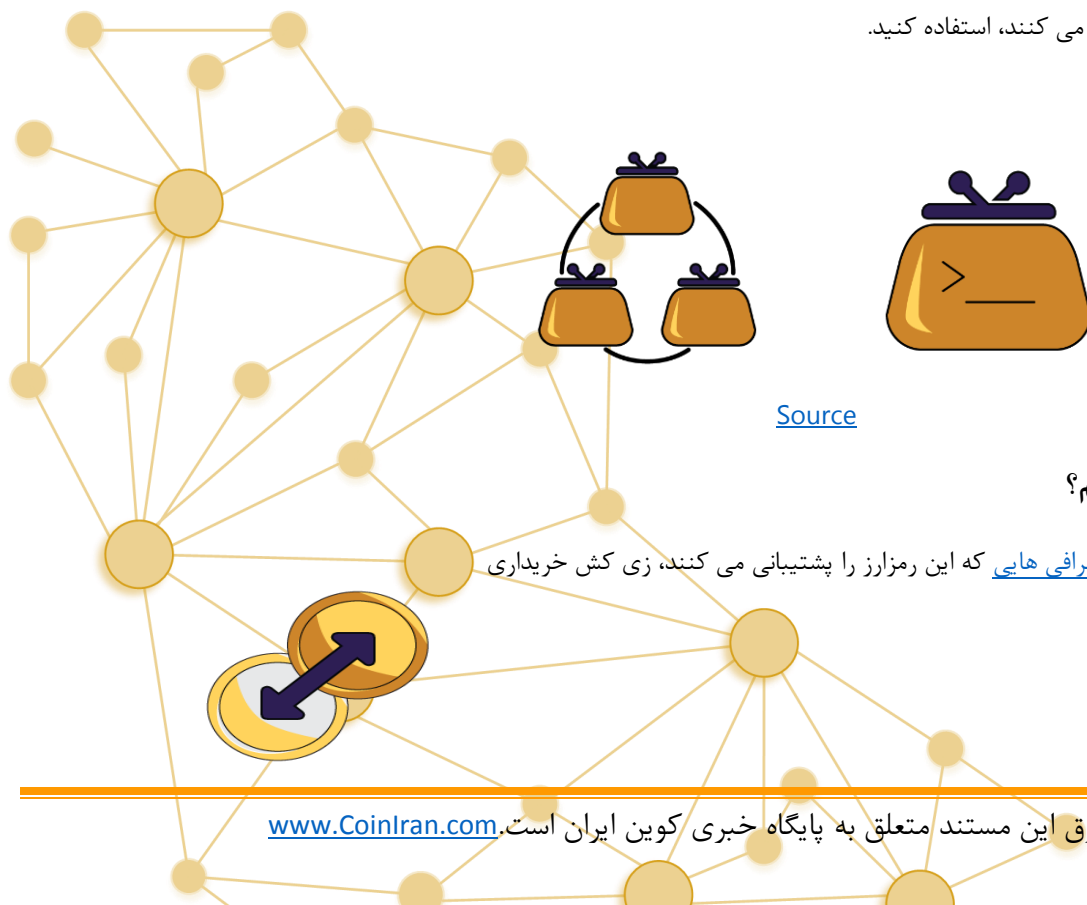
تلاش تیم زی کش بر آن بوده است که جدای از پروتکل خصوصی، تا جایی که ممکن است از ایجاد تغییرات گسترده در طراحی بیت کوین به جز در مواردی منطقی خودداری کنند. اگر علاقه مند به دانستن تغییرات جزئی تکنیکال این دو رمزارز هستید، بر روی این [لینک](#) کلیک کنید.



[Source](#)

انتخاب والت زی کش:

برای نگهداری زی کش هایی که به دست می آورید، می توانید از نسخه رسمی مشتریان زی کش بر روی [Linux](#) یا از بسیاری از [والت](#) های طرف سومی که از این رمزارز پشتیبانی می کنند، استفاده کنید.



[Source](#)

چگونه زی کش به دست آوریم؟

1. شما می توانید به صورت آنلاین از [صرافی هایی](#) که این رمزارز را پشتیبانی می کنند، زی کش خریداری کنید.



[Source](#)

2. دومین راه، استخراج زی کش است که در مقالات مختلفی از کوپین ایران به آن ها پرداخته شده است و شما می توانید با مراجعه به آن ها نحوه استخراج این رمزارز را آموزش ببینید:

الف) استخراج زی کش با یک [کامپیوتر ویندوزی](#) (با استفاده از Claymore و Nicehash)

ب) استخراج زی کش با استفاده از CPU و GPU ([بخش اول](#) و [بخش دوم](#))



[Source](#)

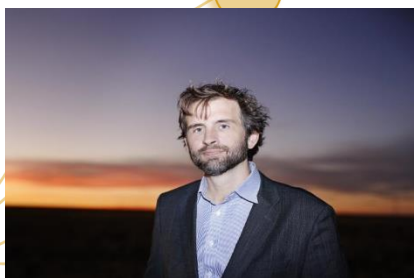
3. سومین راه، دریافت پرداخت های مرتبط با کسب و کارتان به زی کش است که در این صورت برای کسب اطلاعات می توانید با تیم پشتیبانی زی کش [تماس](#) بگیرید.



[Source](#)

تیم زی کش:

مؤسس و مدیر عامل این [تیم Zooko Wilcox](#) است که دارای بیش از بیست سال سابقه در زمینه سیستم های غیر متمرکز و باز، رمزنگاری، امنیت اطلاعات و نیز سابقه همکاری با استارت آپ های مختلف می باشد.



شما می توانید برای مشاهده سایر اعضای این تیم و سوابق کاری آن ها، بر روی این [لینک](#) کلیک نمایید.

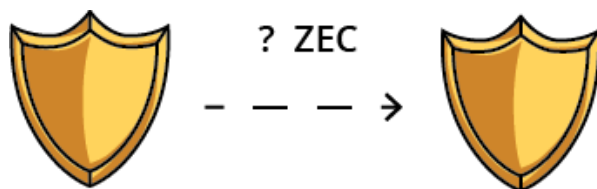


آیا واقعا زی کش حافظ حریم شخصی است؟

چندی پیش محققین کالج لندن با انتشار [مقاله](#) ای، ناشناس بودن رمزارز زی کش را زیر سوال بردند و مدعی شدند که این رمزارز چندان حافظ حریم شخصی نیست. بنا بر اظهارات آنان اگر چه تراکنش های Zcash می تواند محرمانه باشد، اما انتخاب برخی از الگو های تراکنش توسط کاربران نیز همواره می تواند موجب کاهش محرمانگی تراکنش ها گردد.

پاسخ بنیان گذار زی کش در این خصوص به این [شرح](#) بود:

این تحقیق شیوه ای متفاوت از نفوذ به دیوار حریم شخصی شما و طرف مقابل تراکنش را به تصویر می کشد. به این ترتیب که اگر شخصی مقداری ارز از آدرسی شفاف به آدرسی محفوظ ارسال نماید، و آدرس محفوظ بخشی از این دریافتی را به آدرس شفاف دیگری منتقل کند، محرمانگی به خطر خواهد افتاد. اما این تحقیق تکنیک هایی جدید را شامل می شود که می تواند به شکلی مبتکرانه الگو های تراکنش های «نامحفوظ به محفوظ به نامحفوظ» را، درست نقطه مقابل آنچه تحلیل قبلی ارائه نموده بود، به هم ارتباط دهد.



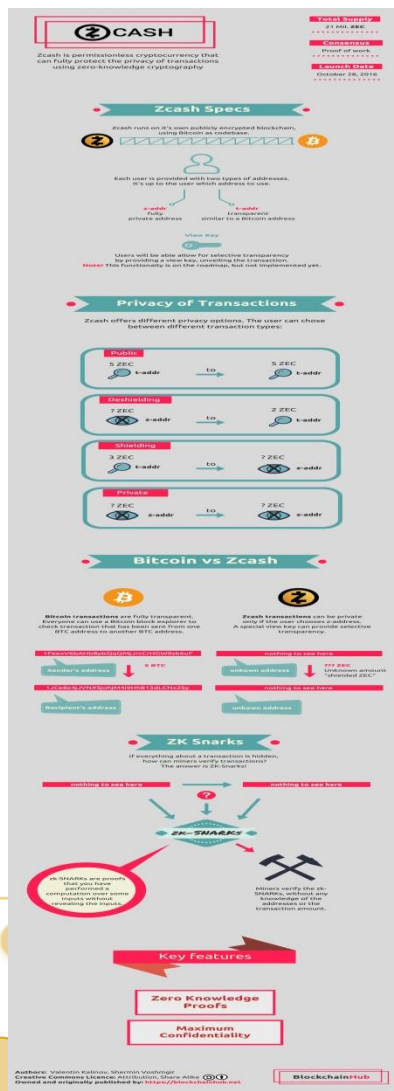
قیمت زی کش:

در لحظه نگارش این مقاله و به نقل از coinmarketcap.com در 17 خرداد 97، هر زی کش با افزایش 0.43 درصدی، 237.33 دلار آمریکا معادل 0.03080190 بیت کوین ارزش دارد. این در حالی است که در این لحظه بیت کوین کاهش 0.68 درصدی ارزش خود را تجربه می کند.

گنجایش بازار (Market Cap) این رمزارز در این لحظه برابر با 969,367,699 دلار آمریکا معادل 125,811 بیت کوین بوده و حجم معاملاتی آن در 24 ساعت گذشته 57,658,000 دلار آمریکا و معادل 7,483 بیت کوین می باشد. میزان زی کش در گردش نیز در این لحظه برابر با 4,084,506 ZEC است.



در پایان، نگاهی به [Infographic](#) این رمزارز می اندازیم تا طرز کار آن و تفاوت های آن با بیت کوین را در قالب تصویر مشاهده کنیم.



توجه!

دیدگاه هایی که در این مقاله ارائه شده اند، متعلق به نویسنده می باشند و لزوماً مربوط به Coiniran نمی باشد و نباید به آن نسبت داده شود.

منابع:

<https://en.wikipedia.org/wiki/Zcash>



<https://en.wikipedia.org/wiki/Zerocoin>

<https://z.cash/fr/blog/anatomy-of-zcash.html>

<https://z.cash/about.html>

<http://zerocoin.org>

coiniran.com

coinmarketcap.com

