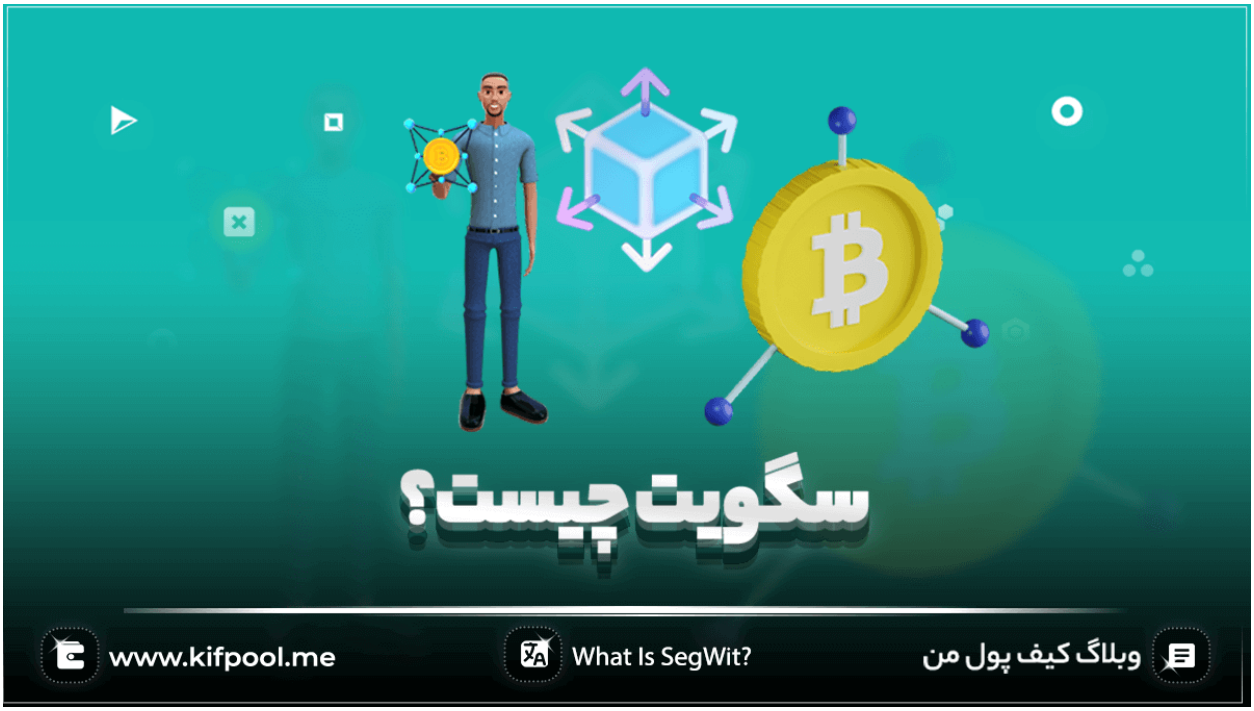



# سگویت چیست؟

این نکته بر کسی پوشیده نیست که برای تجربه یک ترید موفق و دستیابی به تحلیل‌های درست از وضعیت رمزارزها، باید اطلاعات جامعی در ارتباط با اکوسیستم کریپتوکارنسی داشته باشید. یکی از موضوعات و مسائلی که همواره از آن به عنوان معضلی برای رشد و توسعه استفاده از فناوری بلاک چینی یاد می‌شود، به مسئله مقیاس‌پذیری این شبکه‌ها مربوط است. تاکنون شبکه‌های بلاک چینی با انجام به‌روزرسانی‌های مختلف تلاش نموده‌اند تا وضعیت مقیاس‌پذیری (Malleability) را بهبود بخشیده و ظرفیت بلاک‌ها (Block Capacity) را افزایش دهند. در آگوست سال 2017 بود که توسعه‌دهندگان شبکه بلاک چینی بیت کوین برای دستیابی به دو هدف یاد شده به سراغ سافت فورکی به نام **سگویت** (**SegWit**) رفتند.

به نظر بسیاری از صاحب نظران حوزه کریپتوکارنسی، از سگویت می‌توان به عنوان راه‌کاری نویدبخش در حوزه مقیاس‌پذیری این شبکه یاد کرد و افزایش میانگین معاملات به وسیله سگویت سبب شده تا بسیاری از پلتفرم‌ها و شبکه‌های بلاک چینی به استفاده از این فناوری نوین روی آورند. مسلما این سطح از کارایی موجب شده تا ابهامات زیادی در ارتباط با ماهیت و نحوه عملکرد سگویت در ذهن مخاطبان شکل بگیرد و به همین علت ما این مقاله از بلاگ کیف پول من را به معرفی و بررسی دقیق این مفهوم اختصاص داده‌ایم؛ اگر شما هم در این زمینه کنجکاو هستید، تا انتهای این مطلب با ما همراه باشید.

# تاریخچه شکل‌گیری سگویت (SegWit)


قبل از آن که به بررسی ماهیت سگویت بپردازیم، لازم است که به چرایی شکل‌گیری این مفهوم و ضرورت وجودی آن برای شبکه بلاک چینی بیت کوین نگاهی داشته باشیم تا با دیدی بازتر بتوانید مطالبی را که در ادامه به آن‌ها پرداخته خواهد شد را مطالعه نمایید. همان طور که می‌دانید بلاک چین بیت کوین در واقع از زنجیره‌ای از بلاک‌ها شکل گرفته است که بر روی یک بستر آزاد توزیع شده‌اند و از الگوریتم انجام معاملات همتا به همتا (P2P) برای انجام تراکنش‌ها بهره می‌گیرد. هر یک از تراکنش‌های موجود در این شبکه، دارای ورودی و خروجی مشخصی بوده که خروجی آن همان آدرس عمومی گیرنده در این بلاک چین و ورودی آن نیز آدرس عمومی فرستنده است.

به همراه آدرس عمومی فرستنده در بخش ورودی، قسمتی نیز به امضا تراکنش اختصاص داده شده که کاربرد این امضا در زمینه تائید میزان دارایی فرستنده است؛ به بیان بهتر، این امضا (که حجم قابل توجهی از تراکنش را به خود اختصاص می‌دهد) دارایی فرستنده به اندازه مبلغ تراکنش را تائید می‌کند و تضمین می‌دهد که انجام تراکنش بدون مواجهه با مشکل خاصی صورت خواهد گرفت. حال مسئله‌ای که گریبان‌گیر شبکه بلاک چینی بیت کوین شده و آن را به سمت **سگویت** هدایت کرده است، به این واقعیت برمی‌گردد که حجم بلاک‌ها در این شبکه،

پاسخگوی نیاز شبکه بلاک چین بیت کوین نبوده و مشکلات متعددی را به لحاظ مقیاس‌پذیری برای آن به ارمغان آورده است.

با یک حساب سرانگشتی می‌توان به این واقعیت اذعان داشت که با محبوبیت روزافزون استفاده از شبکه بلاک چینی بیت کوین، بلاک‌های این شبکه به سرعت اشغال شده و حجم 1 مگابایتی بلاک‌ها پاسخگوی نیاز روز این شبکه نیست و همین مسئله روند تائید تراکنش‌ها را بسیار کند کرده است؛ امری که چندان خوشایند نبوده و می‌توان از آن به عنوان سدی در برابر رشد استفاده حداکثری از فناوری بلاک چین یاد کرد. لازم به ذکر است که شکل‌گیری صف انتظار برای تائید تراکنش‌ها که گاها ممکن است چندین روز به طول انجامد، تنها ره‌آورد این حجم محدود بلاک‌ها برای این شبکه نبوده و افزایش کارمزد تراکنش‌ها مسئله‌دیگری است که در نتیجه ترافیک سنگین شبکه با آن مواجه خواهیم شد.

## مطلب پیشنهادی: کارمزد در شبکه بلاکچین چگونه محاسبه میشود؟

در پی چنین کشمکش‌های درون شبکه‌ای، دولوپرهای بیت کوین کور، ایده سگویت را مطرح کردند. در واقع این ایده برای اولین بار در دسامبر سال 2015 در کنفرانس مقیاس‌پذیری بیت کوین به وسیله فردی به نام پیتر ویول (Pieter Wiulle) مطرح گردید و حدودا دو سال بعد از ارائه آن، این ایده برای اولین بار در 10 می سال 2017 بر روی شبکه لایت کوین پیاده‌سازی شد و پس از اطمینان از نتیجه‌بخش بودن آن در تاریخ 23 آگوست سال 2017 بر روی شبکه بلاک چینی بیت کوین نیز اعمال گردید.

## آشنایی با مفهوم راهکار سگویت

گفته شد که در حالت عادی، حداکثر اندازه بلاک‌ها در شبکه بیت کوین، 1 مگابایت است و مشکلات مربوط به مقیاس‌پذیری سبب شده تا رشد بالقوه بیت کوین متوقف گردیده و به عنوان سدی محکم در برابر تبدیل شدن آن به یک سیستم پرداخت با حجم تراکنش‌های بالا عمل نماید.
راهکار **سگویت** (SegWit) که در واقع کوتاه شده عبارت «Segregated Witness» است، یک به‌روزرسانی کاربردی بوده که سبب شده تا اندازه تراکنش‌ها در شبکه بیت کوین سبک‌تر گردد.
بررسی لغوی این اصطلاح اطلاعات خوبی را در اختیار ما قرار می‌دهد تا بررسی نحوه عملکرد این راهکار کاربردی را با بیان ساده‌تر و قابل درک‌تر پیش ببریم؛ کلمه «Segregated» به معنای تفکیک و واژه «Witness» نیز به معنای شاهدان (که در شبکه بلاک چینی منظور از آن همان امضای تراکنش‌هاست) می‌باشد که در معنای اصطلاحی می‌توان این عبارت لاتینی را به معنای جداسازی امضاهای تراکنش ترجمه نمود.

در واقع در راهکار سگویت، ما با حذف اطلاعات مربوط به امضای تراکنش‌ها و ذخیره‌سازی آن در خارج از بلاک تراکنش مبنا روبه‌رو هستیم که سگویت با چنین کاری، انعطاف‌پذیری تراکنش را اصلاح می‌نماید. لازم به ذکر است که هرچند با اعمال راهکار سگویت بر تعداد تراکنش‌های موجود در هر بلاک افزوده می‌شود؛ اما نباید این نکته را از نظر دور داشت که هدف اولیه این به‌روزرسانی در برطرف کردن باگ موجود در کد بیت کوین مربوط به انعطاف‌پذیری تراکنش بوده است. این باگ این امکان را برای کاربران شبکه فراهم می‌کرد تا جزئیات کوچکی را تغییر دهند که چنین امری منجر به تغییر ID تراکنش می‌گردید، البته محتوای تراکنش بدون تغییر باقی می‌ماند.

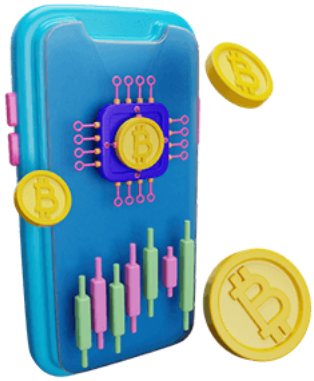
هرچند که این نقص و باگ، مشکل چندان حادی را در امنیت شبکه بیت کوین ایجاد نمی‌کرد؛ اما مانع توسعه ویژگی‌های پیچیده شبکه نظیر استفاده از قراردادهای هوشمند (Smart Contracts) و پروتکل‌های لایه 2 می‌گردید. حال با اعمال راهکار سگویت به راحتی می‌توان امضاها و اسکریپت‌ها را بدون آن که تغییری در ID تراکنش ایجاد گردد، تغییر داد. برای درک بهتر اهمیت چنین به‌روزرسانی با یک مثال عملی توضیحات خود را ادامه می‌دهیم:

تصور کنید فردی به نام علی باید 4 بیت کوین به فرد دیگری به نام رضا پرداخت نماید. در مثال ما رضا قصد کلاهبرداری از علی را داشته و می‌خواهد علی را فریب داده و به جای 4 بیت کوین، 8 بیت کوین از وی دریافت کند و به همین علت اطلاعات امضای مربوط به تراکنش علی را قبل از تائید تغییر می‌دهد که در نتیجه چنین کاری ID تراکنش (بدون برجای گذاشتن هیچگونه تغییر خاصی در خود تراکنش)، تغییر می‌کند. حال رضا 4 بیت کوین را دریافت می‌کند و شبکه نیز پس از آن که تراکنش اصلاح شده را تائید نمود، تراکنش اصلی را لغو می‌کند و در همین نقطه است که رضا به علی می‌گوید 4 بیت کوین را دریافت نکرده و علی نیز متوجه می‌شود که تراکنش اصلی انجام نشده و برگشته است. در چنین حالتی علی مجددا 4 بیت کوین دیگر به رضا ارسال می‌کند.

در راهکار مورد ارائه موسوم به **سگویت**، اطلاعات امضای تراکنش از بلاک تراکنش مبنا جدا شده و یک زنجیره جانبی، مستقل و خارج از شبکه بلاک چینی به منظور ذخیره‌سازی چنین داده‌هایی ایجاد می‌نماید تا به این ترتیب مانع سواستفاده کلاهبردارانی همچون رضا از این نقص گردیده و اجازه ندهد که این افراد ID تراکنش را تغییر دهند.

**مطلب پیشنهادی: روش های کاهش کارمزد تراکنش های بیت کوین**

## نحوه عملکرد راهکار سگویت

احتمالا با مطالعه مطالب فوق، یک تصویر کلی از نحوه بهبود میزان مقیاس‌پذیری شبکه به وسیله طرح **سگویت** در ذهن شما شکل گرفته است؛ اما در این بخش از مقاله کیف پول من قصد داریم که به طور تفصیلی و دقیق‌تر به این سوال که «طرح سگویت چگونه توانسته است ظرفیت بلاک‌ها را در بلاک چین بیت کوین افزایش دهد؟» پاسخ دهیم. به طور کلی این راهکار با استفاده از دو روش افزایش آنی حجم بلاک تا 4 مگابایت و جداسازی امضا از تراکنش به هدف خویش در زمینه افزایش حجم بلاک‌های بیت کوین جامه عمل پوشانیده است که در ادامه به بررسی تفصیلی هر یک از موارد گفته شده می‌پردازیم:

**افزایش حجم بلاک**

طرح سگویت قادر است سایز هر بلاک را از 1 مگابایت تا 4 مگابایت افزایش دهد که این میزان متناسب با شرایط کلی هر شبکه متفاوت بوده و به نظر صاحب‌نظران این حوزه، پس از فعالسازی سگویت، سایز بلاک‌ها بلافاصله در محدوده 2 الی 2.1 مگابایت قرار می‌گیرد. علت این افزایش سایز بلاک‌ها در این نکته نهفته است که هر بایت در تراکنش‌هایی که طرح سگویت در آن‌ها فعال گردیده، برابر با 1 واحد وزنی می‌باشد و این در حالی است که در حالت معمول، این میزان برابر با 4 واحد است.

طبیعتا به هنگامی که با استفاده از سگویت، بخشی از داده‌ها از بلاک اصلی و پایه منفک می‌گردند، به میزان 4 برابر آن مقدار، فضای خالی در بلاک مورد نظر ایجاد می‌گردد. به بیان ساده‌تر،

با استفاده از سگویت، هر بایت اطلاعاتی صرفا یک چهارم از حجم بلاک را اشغال می‌کند و فضای ذخیره‌سازی تراکنش‌ها در چنین بلاک‌هایی 4 برابر افزایش می‌یابد.

## مطلب پیشنهادی: امنیت شبکه بلاکچین

**خارج کردن امضاها از ورودی تراکنش**

به هنگامی که از داده بلاک‌ها سخن به میان می‌آید، محال ممکن است که اسمی از درخت مرکل وارد بحث نگردد! ریشه درخت مرکل که در واقع اوج هرم مرکل را شکل داده، ساختاری است که این امکان را برای بلاک‌ها فراهم می‌آورد تا تراکنش‌ها را بدون نیاز به به بررسی حجم بالایی از داده تراکنش‌ها، صحت‌سنجی و تائید نمایند. با اعمال راهکار **سگویت**، اطلاعات مربوط به امضا دیگر بخشی از شناسه تراکنش به شمار نمی‌روند؛ اما همچنان در تراکنش گنجانده می‌شوند تا بلاک از اعتبار ساقط نگردد. مسلما با توجه به چنین توضیحی، این واقعیت بر همه نمایان می‌گردد که بایستی یک درخت مرکل جداگانه‌ای برای داده‌های مربوط به امضای تراکنش شکل بگیرد. به بیان ساده‌تر، با استفاده از طرح سگویت، داده‌های مربوط به امضای تراکنش در یک بخش مستقل و در انتهای بلاک قرار می‌گیرند و به این ترتیب روند محاسبه شناسه تراکنش را سرعت می‌بخشند.

## سگویت؛ راهکاری موثر در زمینه برطرف ساختن مشکلات مربوط به مقیاس‌پذیری بلاک چین

هرچند که اعمال طرح **سگویت** در سال 2017 نارضایتی‌هایی را در میان اعضای جامعه بیت کوین ایجاد نمود و منجر به فورک شبکه به بیت کوین کش و دو نیم شدن جامعه بیت کوینی گردید؛ اما نباید از این واقعیت چشم‌پوشی کرد که شبکه بلاک چین بیت کوین همواره به دنبال راه‌حلی برای مشکل مقیاس‌پذیری خود بوده و به نحوی قصد دارد خود را به عنوان یک شبکه فعال در حوزه پردازش تراکنش‌ها آن هم در مقیاس بالا نشان دهد تا جایگاه خود را در سیستم نقل و انتقالات مالی تثبیت نماید.

با توجه به تاثیر راهکار سگویت در ارتقا مقیاس‌پذیری شبکه بلاک چین بیت کوین، ما این مقاله از بلاگ کیف پول من را به معرفی و بررسی دقیق ماهیت و چیستی طرح سگویت اختصاص دادیم و همان طور که در مطالب فوق مشاهده کردید، این طرح منجر به بالا رفتن تعداد تراکنش‌ها در بلاک گردیده و مقیاس‌پذیری شبکه را بهبود می‌بخشد. این طرح در واقع با جداسازی امضا تراکنش‌ها که حجم قابل توجهی از بلاک‌ها را به خود اختصاص می‌دهند، بر این هدف خویش جامه عمل پوشانیده و نه تنها سرعت تائید تراکنش‌ها را در شبکه بلاک چین بیت کوین بهبود بخشیده، بلکه تاثیر مثبتی نیز بر روند کاهشی کارمزدها در این شبکه داشته است. ناگفته نماند که اگر در ارتباط با مفهوم راهکار سگویت سوالی دارید که در این مقاله به پاسخ این سوال

اشاره‌ای نشده است، می‌توانید سوال خود را در بخش نظرات با ما در میان بگذارید تا کارشناسان ما در اسرع وقت به سوال شما پاسخ دهند.