



# سپیدنامه ریال اتریوم

اسفند ۲۵۸۴ شاهنشاهی

## مقدمه

ریال اتریوم یک توکن دیجیتال غیرمتمرکز بر بستر اتریوم است که با هدف ایجاد کنترل واقعی و کامل بر پول برای ایرانیان طراحی شده است. این سیستم به طور کامل روی بلاکچین اتریوم اجرا می‌شود و از طریق یک قرارداد هوشمند غیرقابل تغییر عمل می‌کند که نقش یک صندوق شفاف را ایفا می‌نماید. هر فردی در هر نقطه از جهان می‌تواند با ارسال اتریوم به این قرارداد، به صورت آنی و بر اساس قیمت روز بازار، توکن ریال اتریوم دریافت کند. به همین شکل، کاربران می‌توانند در هر زمان توکن‌های خود را به قرارداد بازگردانند و معادل آن اتریوم دریافت نمایند. تمامی این فرآیندها به صورت خودکار انجام می‌شود و هیچ بانک، دولت یا نهاد مرکزی در آن دخالتی ندارد. هدف این پروژه ایجاد یک ریال دیجیتال است که هیچ قدرتی نتواند آن را مسدود، مصادره یا سانسور کند. کل

ذخیره اتریوم که پشتوانه این سیستم را تشکیل می‌دهد، در داخل قرارداد هوشمند نگهداری می‌شود و تمامی قوانین توسط کدی اجرا می‌شوند که به صورت دائمی روی بلاک‌چین ثبت شده است. به این ترتیب، یک نظام پولی مبتنی بر بازار آزاد شکل می‌گیرد که در آن پول توسط بازار آزاد حمایت می‌شود و نه دولت.

## مشکلی که حل می‌کنیم

در طول دهه‌های گذشته، سیستم بانکی ایران به طور کامل تحت کنترل حکومت بوده است. بانک‌ها می‌توانند بدون اطلاع قبلی حساب‌ها را مسدود کنند، محدودیت‌های روزانه تعیین نمایند، انتقال‌ها را با تأخیر انجام دهند و تمامی فعالیت‌های مالی را تحت نظارت داشته باشند. در شرایطی مانند اعتراضات، تحریم‌ها، جنگ یا قطع اینترنت، دسترسی مردم به دارایی‌هایشان ممکن است به طور کامل از بین برود. حتی در شرایط عادی نیز، وجود احراز هویت و نظارت دائمی به حکومت این امکان را می‌دهد که در هر زمان دارایی افراد را مصادره کند. در چنین سیستمی، پول عملاً در مالکیت واقعی مردم نیست، بلکه تحت کنترل ساختار حاکم قرار دارد. ریال اتریوم این وضعیت را تغییر می‌دهد و با انتقال فرآیند پولی به شبکه اتریوم، مالکیت واقعی را به کاربران بازمی‌گرداند. در این مدل، کیف پول هر فرد به بانک شخصی او تبدیل می‌شود و هیچ‌کس خارج از اختیار او نمی‌تواند به دارایی‌اش دسترسی داشته باشد.

## نحوه کار سیستم

فرآیند استفاده از ریال اتریوم ساده و مستقیم طراحی شده است. برای خرید، کاربر مقدار دلخواهی از اتریوم را به آدرس **buy.rial.eth** ارسال می‌کند. قرارداد هوشمند قیمت روز بازار را از منبع قیمت دریافت کرده، کارمزد اندکی معادل ۰.۱ درصد را کسر می‌کند و بلافاصله مقدار معادل توکن را در کیف پول کاربر ایجاد می‌نماید. اتریوم ارسال شده در داخل قرارداد باقی می‌ماند و به‌عنوان پشتوانه توکن‌های جدید عمل می‌کند.

برای فروش، کاربر می‌تواند توکن‌های خود (ریال) را به آدرس **sell.rial.eth** یا مستقیماً به آدرس قرارداد ارسال کند. قرارداد هوشمند به صورت خودکار توکن‌های دریافتی را از بین می‌برد و معادل اتریوم آن را، پس از کسر کارمزد ۰.۱ درصد، به کیف پول کاربر بازمی‌گرداند.

برای انجام این فرآیند نیازی به نرم‌افزار یا رابط کاربری خاصی وجود ندارد و این عملیات با استفاده از کیف پول‌های معمولی مانند Trust Wallet یا MetaMask نیز قابل انجام است.

## سازوکار پشتوانه و صندوق

هر واحد ریال اتریوم با اتریوم واقعی که در داخل قرارداد هوشمند نگهداری می‌شود پشتیبانی می‌گردد. این ذخیره به‌گونه‌ای در قرارداد قفل شده است که هیچ فردی، حتی سازندگان پروژه، امکان برداشت یا جابجایی آن را ندارند.

قرارداد به‌طور مداوم نسبت میان ذخیره اتریوم و تعداد توکن‌های در گردش را بررسی می‌کند. هدف سیستم این است که ارزش هر توکن در حدود یک ریال باقی بماند.

در صورتی که به هر دلیل نسبت پشتوانه کمتر از مقدار لازم برای پوشش کامل عرضه در قیمت بازار شود، قرارداد به‌صورت خودکار وارد حالت بازخرید نسبی می‌شود. در این حالت، زمانی که کاربری ریال خود را برای دریافت اتریوم ارسال می‌کند، سهمی منصفانه از کل ذخیره باقی‌مانده اتریوم دریافت خواهد کرد. این سهم به‌طور برابر میان تمامی دارندگان توکن تقسیم می‌شود. این مکانیزم به‌صورت فوری فعال می‌شود و نیازی به کاهش شدید قیمت اتریوم ندارد. هدف از این سازوکار، حفظ پایداری سیستم و جلوگیری از ورشکستگی در هر شرایطی است.

## کارمزدها و اقتصاد سیستم

تنها کارمزد موجود در این سیستم، کارمزدی معادل ۰.۱ درصد برای هر تراکنش خرید یا فروش است. این کارمزد به تأمین هزینه‌های توسعه و پایداری پروژه کمک می‌کند. انتقال توکن بین کاربران هیچ کارمزدی ندارد و تنها هزینه مربوط به کارمزد شبکه اتریوم است.

راه‌اندازی این پروژه به‌صورت کاملاً عادلانه انجام شده است. هیچ توکنی از پیش استخراج نشده، هیچ سهمی به تیم یا سرمایه‌گذاران اختصاص نیافته و تمامی توکن‌های موجود صرفاً از طریق پرداخت اتریوم توسط کاربران واقعی ایجاد شده‌اند. نام توکن در کیف پول‌ها و مرورگرهای بلاک‌چین، Riale Bazaar Azad با نماد RIALE است.

## ریسک‌ها و شفافیت کامل

ما بر این باوریم که هر کاربر باید پیش از استفاده، تمامی ریسک‌های این سیستم را به‌طور کامل درک کند.

1. به دلیل وجود فیلترینگ و تحریم‌ها در ایران، دسترسی به کیف پول و انجام تراکنش‌ها معمولاً نیازمند استفاده از یک VPN پایدار است. در صورت قطع کامل اینترنت، ممکن است دسترسی موقت به دارایی‌ها امکان‌پذیر نباشد، هر چند توکن‌ها همچنان به‌طور کامل روی بلاک‌چین امن باقی می‌مانند.
2. در دنیای رمزارزها، هر کاربر مسئول کامل دارایی خود است. در صورت از دست دادن کلید خصوصی یا عبارت بازیابی، هیچ راهی برای بازیابی دارایی وجود ندارد و این مسئولیت به‌صورت دائمی بر عهده کاربر خواهد بود.
3. تمامی تراکنش‌ها نیازمند پرداخت کارمزد شبکه اتریوم هستند و کاربران باید همواره مقدار کمی اتریوم برای این منظور در اختیار داشته باشند.
4. قیمت خرید ریال از شما به‌طور مستقیم به میزان اتریوم موجود در قرارداد وابسته است. در صورت کاهش قیمت اتریوم نسبت به ریال، قرارداد به‌صورت خودکار نرخ بازخرید را بر اساس مکانیزم نسبی

تنظیم می‌کند. در این شرایط ممکن است کاربر اتریوم کمتری نسبت به قیمت بازار دریافت کند، اما این سازوکار از فروپاشی سیستم جلوگیری کرده و همه کاربران را به طور برابر محافظت می‌کند.

5. شبکه اتریوم یک بلاک‌چین عمومی است و تمامی تراکنش‌ها و موجودی‌ها برای همه قابل مشاهده هستند. در صورتی که هویت واقعی کاربر به آدرس کیف پول او مرتبط شود، حریم خصوصی وی ممکن است تحت تأثیر قرار گیرد.

6. منبع قیمت فعلی به صورت متمرکز اداره می‌شود و مهم‌ترین فرض اعتماد در این سیستم محسوب می‌گردد. در صورتی که این بخش دچار نفوذ، دستکاری یا اختلال شود، یک مهاجم می‌تواند مقدار نامتناسبی از توکن‌ها را ایجاد کرده و به طور بالقوه بخش عمده یا حتی کل ذخیره اتریوم را از سیستم خارج کند. برای توضیحات کامل، به بخش «ریسک نفوذ به اوراکل» مراجعه کنید.

## ریسک نفوذ به اوراکل

در وضعیت فعلی، سیستم ریال اتریوم برای تعیین نرخ تبدیل بین اتریوم و ریال به یک منبع قیمت خارجی (اوراکل) وابسته است. این منبع قیمت از طریق یک سرور که تحت کنترل تیم پروژه است تأمین می‌شود. در حالی که قرارداد هوشمند و ذخیره اتریوم به طور کامل غیرمتمرکز هستند و هیچ کس امکان تغییر یا دسترسی به آن‌ها را ندارد، اوراکل همچنان یک جزء متمرکز باقی می‌ماند و مهم‌ترین فرض اعتماد در کل سیستم محسوب می‌شود.

در صورتی که اوراکل دچار نفوذ شود—چه از طریق هک شدن، افشای کلید خصوصی، یا سوءنیت اپراتور—امکان دستکاری داده‌های قیمتی ارسال شده به قرارداد فراهم می‌شود. از آنجا که قرارداد به طور کامل به این داده‌ها اعتماد می‌کند، هر مقدار نادرستی مستقیماً در فرآیند ایجاد (mint) و بازخرید (redeem) توکن‌ها استفاده خواهد شد.

برای درک شدت این ریسک، می‌توان یک سناریوی حمله مهم را در نظر گرفت. فرض کنید مجموع عرضه ریال اتریوم برابر با یک هزار میلیارد ریال باشد که توسط مقدار متناظری اتریوم در قرارداد پشتیبانی می‌شود. اگر یک مهاجم کنترل اوراکل را به دست بگیرد، می‌تواند قیمت اتریوم را به صورت مصنوعی بسیار بالا اعلام کند؛ برای مثال، گزارش دهد که هر ۱ اتریوم برابر با ۱۰۰ هزار میلیارد ریال است. در این حالت، مهاجم می‌تواند با ارسال مقدار بسیار کمی اتریوم (مثلاً ۱ اتریوم) به قرارداد، حجم عظیمی از توکن‌ها را دریافت کند و عملاً با هزینه‌ای ناچیز، مالک بخش عمده‌ای از کل عرضه شود.

پس از به دست آوردن این سهم غالب، مهاجم می‌تواند دستکاری را معکوس کرده و قیمت را به مقدار واقعی یا حتی بسیار پایین بازگرداند. در این مرحله، سیستم تشخیص می‌دهد که ذخیره موجود برای پشتیبانی از کل توکن‌ها در قیمت اعلام شده کافی نیست و به صورت خودکار وارد حالت بازخرید نسبی می‌شود. در این حالت، هر توکن نمایانگر سهمی از کل ذخیره اتریوم خواهد بود.

از آنجا که مهاجم اکنون مالک بخش عمده‌ای از توکن‌هاست، می‌تواند آن‌ها را بازخرید کرده و سهم متناسبی از اتریوم موجود در قرارداد را برداشت کند—که این مقدار می‌تواند تقریباً کل ذخیره را شامل شود. سایر کاربران همچنان توکن‌های خود را در اختیار خواهند داشت، اما اتریوم بسیار کمی در قرارداد باقی خواهد ماند و عملاً امکان بازخرید مؤثر از بین می‌رود.

نکته مهم این است که در این سناریو، قرارداد هوشمند دچار نقص نشده و هیچ یک از قوانین نقض نمی‌شوند. سیستم دقیقاً مطابق طراحی خود عمل می‌کند، اما بر پایه داده‌های قیمتی نادرست. آسیب‌پذیری صرفاً از ماهیت متمرکز اوراکل ناشی می‌شود.

این بدان معناست که در بدترین حالت، در صورت نفوذ یا سوءاستفاده از اوراکل، از نظر فنی این امکان وجود دارد که یک عامل مخرب بخش عمده یا حتی کل ذخیره اتریوم را از سیستم خارج کند. در این شرایط، توکن‌ها همچنان در کیف پول کاربران باقی می‌مانند، اما پشتوانه آن‌ها به شدت کاهش یافته یا عملاً از بین می‌رود.

ما این ریسک را به‌طور کامل و شفاف بیان می‌کنیم. طراحی فعلی بر سادگی و کارکرد عملی تمرکز دارد، اما این ملاحظه را به‌عنوان یک محدودیت شناخته‌شده در خود دارد. برنامه ما این است که این وابستگی را با جایگزینی اوراکل متمرکز با یک سیستم قیمت‌دهی کاملاً غیرمتمرکز که از چندین منبع مستقل و قابل‌اعتماد استفاده می‌کند، به‌طور کامل حذف کنیم. با پیاده‌سازی این تغییر، هیچ نهاد یا فردی قادر به دستکاری قیمت نخواهد بود و این نوع حمله به‌طور کامل از بین می‌رود.

تا زمان تحقق این هدف، کاربران باید در نظر داشته باشند که اوراکل تنها بخش نیازمند اعتماد در سیستم است و ریسکی سیستمی ایجاد می‌کند که می‌تواند بر کل ذخیره تأثیر بگذارد.

## غیرمتمرکز بودن و امنیت

قرارداد هوشمند این سیستم در بخش‌های اصلی خود غیرقابل تغییر است و حتی سازندگان پروژه نیز نمی‌توانند در عملکرد آن دخالت کنند یا دارایی‌ها را کنترل نمایند. تنها بخش قابل تغییر در حال حاضر آدرس منبع قیمت است که آن نیز می‌تواند با یک تراکنش برای همیشه قفل شود. این قرارداد با استفاده از کتابخانه‌های معتبر OpenZeppelin پیاده‌سازی شده و در برابر حملات رایج محافظت شده است. تمامی قوانین سیستم توسط کدی اجرا می‌شوند که به‌صورت دائمی روی بلاک‌چین اتریوم قرار دارد.

## راه‌اندازی عادلانه و جامعه

ریال اتریوم با رویکردی کاملاً عادلانه راه‌اندازی شده است. هیچ پیش‌استخراجی انجام نشده، هیچ سرمایه‌گذاری اولیه وجود نداشته و هیچ تخصیص پنهانی صورت نگرفته است. این پروژه بر پایه مشارکت جامعه شکل گرفته و

رشد آن وابسته به کاربران است. از همه دعوت می‌شود که با یادگیری، استفاده و اشتراک‌گذاری این سیستم، در تقویت آن نقش داشته باشند. در آینده، برنامه‌هایی برای غیرمتمرکز سازی کامل منبع قیمت در نظر گرفته شده است.

## برنامه‌های آتی

برای گسترش، تقویت و پشتیبانی از اکوسیستم ریال اتریوم، مسیرهای کلیدی متعددی برای توسعه آینده تعریف کرده‌ایم. هدف ما ساخت سیستمی پایدار، جامعه‌محور و واقعاً غیرمتمرکز است که بتواند در طول زمان به یک زیرساخت مالی واقعی تبدیل شود.

اولویت نخست ما رشد ارگانیک کامیونیتی است. این پروژه به افرادی وابسته است که آن را درک می‌کنند و به آن باور دارند. هدف ما این است که اهمیت پول مستقل و غیرمتمرکز و دلیل اهمیت آن را به صورت شفاف منتقل کنیم. حفاظت از حق مالکیت خصوصی، بازار آزاد و حاکمیت مالی فردی از اصول بنیادی این سیستم هستند. آموزش کاربران و گسترش این دیدگاه در جامعه، بخش مهمی از استراتژی ما را تشکیل می‌دهد.

در کنار این موضوع، برنامه داریم برای دریافت گزنت‌ها اقدام کنیم و ارتباطات قوی در اکوسیستم گسترده‌تر بلاک‌چین ایجاد نماییم. با همکاری با پروژه‌ها، سازمان‌ها و مشارکت‌کنندگان مختلف، به دنبال جذب توسعه‌دهندگان، سازندگان و حامیانی هستیم که با چشم‌انداز ایجاد سیستم‌های مالی باز و مستقل همسو باشند.

یکی دیگر از محورهای مهم، افزایش تقاضا برای توکن است. همان‌طور که پیش‌تر توضیح داده شد، در صورت کاهش قیمت اتریوم، میزان پشتوانه موجود در سیستم به صورت نسبی کاهش می‌یابد و ممکن است کاربران مجبور شوند توکن‌های خود را با قیمتی پایین‌تر از نرخ بازار باز خرید کنند. برای کاهش این اثر، لازم است تقاضای کافی در بازار ایجاد شود تا کاربران بتوانند به جای تکیه صرف بر قرارداد، توکن‌های خود را در میان اعضای جامعه یا در بازارهای ثانویه با قیمتی نزدیک‌تر به ارزش واقعی معامله کنند.

در راستای این هدف، از توسعه‌دهندگان دعوت می‌کنیم تا بر بستر اکوسیستم ریال اتریوم، اپلیکیشن‌ها، ابزارها و خدمات مختلف ایجاد کنند. علاوه بر این، تیم پروژه قصد دارد یک صرافی راه‌اندازی کند که امکان تبدیل بین اتریوم و ریال اتریوم را فراهم کند و همچنین امکان معامله قراردادهای آتی مبتنی بر ریال را ارائه دهد. این صرافی با استفاده از مشوق‌هایی برای بازارگردانی طراحی خواهد شد تا جذب حداکثر نقدینگی و کشف قیمت کارآمد را تضمین کند. جزئیات بیشتر این طرح در آینده منتشر خواهد شد.

در بخش فنی، یکی از اولویت‌های اصلی ما حذف وابستگی به اوراکل متمرکز است. در این راستا، در حال بررسی روش‌های مختلفی هستیم، از جمله استفاده از شبکه‌های اوراکل غیرمتمرکز مانند Chainlink، بهره‌گیری از داده‌های قیمتی استخراج‌شده از صرافی‌های غیرمتمرکز (DEX AMM) و مدل‌های ترکیبی که چندین منبع

مستقل را با یکدیگر ترکیب می‌کنند. هدف نهایی، ایجاد یک مکانیزم قیمت‌گذاری کاملاً غیرمتمرکز و مقاوم در برابر دستکاری است.

همچنین در حال بررسی و بهبود منطق قیمت‌گذاری سیستم هستیم. در حال حاضر، قیمت ایجاد (mint) بر اساس نرخ بازار تعیین می‌شود. با این حال، در شرایطی که قیمت بازخرید (redeem) کمتر از قیمت بازار باشد، ممکن است افزایش قیمت ایجاد برای کاهش عرضه مفید باشد. این رویکرد می‌تواند به تقویت تقاضا، بهبود قیمت توکن و حمایت بهتر از دارندگان کمک کند. این بخش همچنان در مرحله تحقیق و توسعه قرار دارد و ما متعهد به یافتن پایدارترین و کارآمدترین طراحی ممکن هستیم.

ما بر این باوریم که موفقیت این پروژه تنها از طریق تلاش جمعی امکان‌پذیر است. از مشارکت، ایده‌ها و همکاری جامعه استقبال می‌کنیم. آینده ریال اتریوم توسط کسانی ساخته خواهد شد که در ساخت، حمایت و توسعه آن مشارکت می‌کنند.

## خلاصه

ریال اتریوم صرفاً یک رمزارز نیست، بلکه راهکاری برای بازگرداندن کنترل پول به مردم است. برای نخستین بار، امکان ایجاد یک ریال دیجیتال فراهم شده که هیچ قدرتی قادر به سانسور، مسدودسازی یا مصادره آن نیست. صندوق این سیستم روی بلاک‌چین قرار دارد، قوانین آن توسط کدی تغییرناپذیر اجرا می‌شوند و کنترل آن به‌طور کامل در اختیار کاربران است.

برای شروع، کافی است اتریوم به آدرس **buy.rial.eth** ارسال کنید و در صورت نیاز، با استفاده از **sell.rial.eth** آن را بازخرید نمایید. این یک گام در جهت ساختن آینده مالی آزاد برای ایران است.

## لینک‌های رسمی

آدرس قرارداد: [0x21c3AA992d0C5929459383d58B73cAAEa0a2584e](https://rialet.com/0x21c3AA992d0C5929459383d58B73cAAEa0a2584e)

وبسایت: <https://rialet.com>

ایمیل: [info@rialet.com](mailto:info@rialet.com)

گیت‌هاب: <https://github.com/rialetthereum/rialet>

ایکس: [@RialEthereum](https://twitter.com/RialEthereum)

تلگرام: [@rialet](https://t.me/rialet)

**هشدار:** این سپیدنامه صرفاً برای اطلاع‌رسانی ارائه شده است. پیش از استفاده از هر پروتکل غیرمتمرکز، لازم است تحقیق کافی انجام دهید و ریسک‌ها را به‌طور کامل درک کنید. این پروژه با هدف شفافیت کامل و ایجاد یک سیستم غیرمتمرکز واقعی برای ایرانیان طراحی شده است. بیاید پول خود را آزاد کنیم.