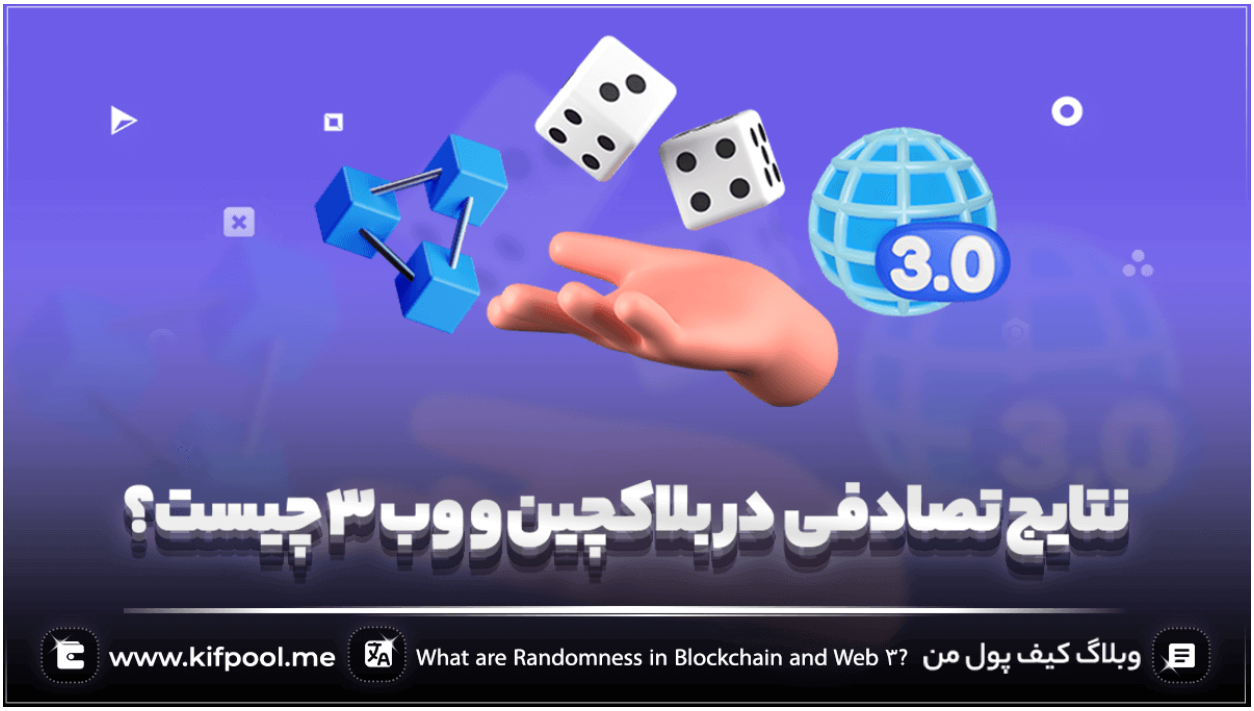
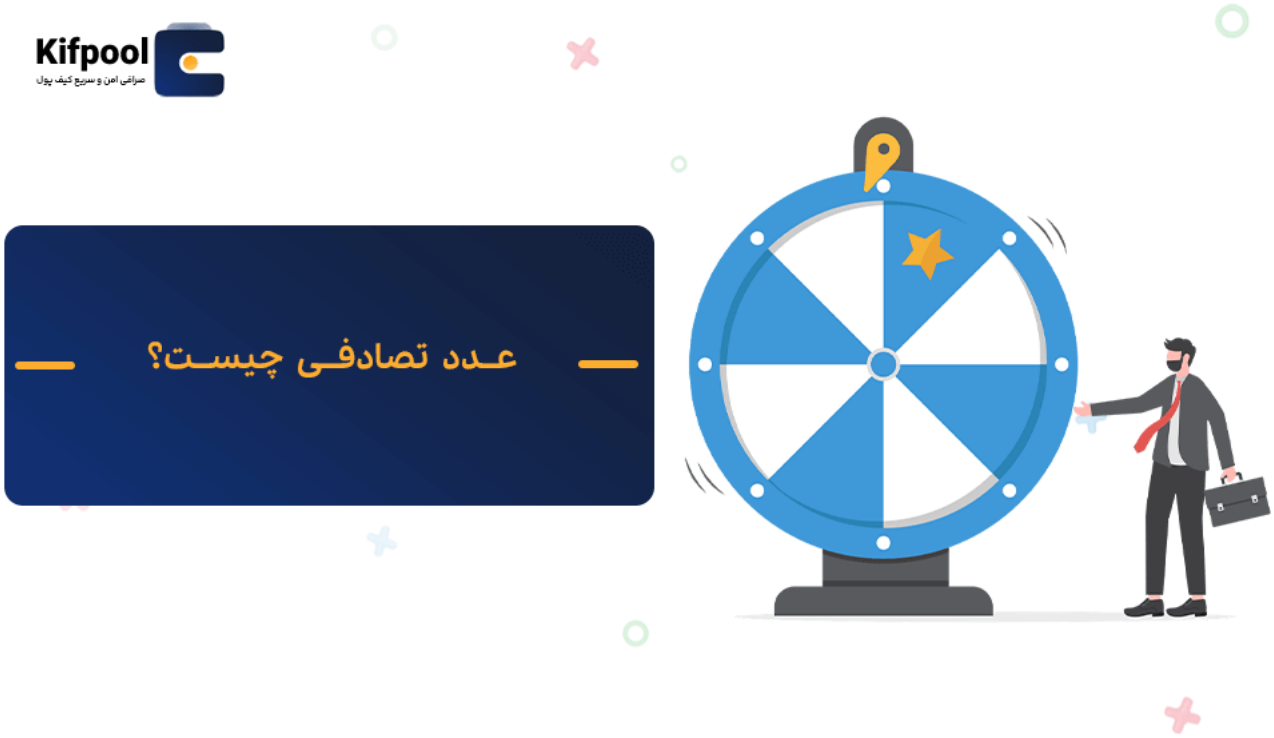


نتایج تصادفی در بلاکچین و وب 3 چیست؟

فناوری بلاکچین به دلیل قدمت کم آن همچنان ابهامات زیادی را در ذهن کاربران ایجاد کرده که استفاده از آن نیازمند داشتن اطلاعات کافی در ارتباط با نحوه عملکرد و همچنین اصطلاحات موجود در آن است. این که بدانیم رمزنگاری نامتقارن بر چه پایه‌ای شکل گرفته، مطمئنا استفاده از آن را برای ما قابل درک‌تر خواهد کرد. یکی از نکات جالبی که کاربران قرن 21 باید به آن توجه داشته باشند این است که بدون اعداد و نتایج تصادفی، بسیاری از تکنولوژی‌های روزمره مورد استفاده ما انسان‌ها از اینترنت و رایانه گرفته تا تلفن‌های همراه شکلی متفاوت‌تر به خود می‌گرفتند.

در واقع با افزایش تعاملات اقتصادی، اجتماعی و فرهنگی، تقاضا برای تصادفی و غیرقابل پیش‌بینی بودن جهان طبیعی بیشتر شده است. تصادفی بودن به معنای فقدان الگویی برای قابل پیش‌بینی بودن بوده و همین معنا در حوزه بلاکچین و وب 3 نیز وارد شده است. با توجه به ماهیت خاص این فناوری نوظهور، بلاک چین نیازمند مکانیسم‌های امنیتی قدرتمند و فرآیند تصمیم‌گیری بی‌طرفانه بوده که چنین چیزی مستلزم وجود نتایج تصادفی و غیرقابل پیش‌بینی است. با توجه به اهمیت این موضوع، تا انتهای این مطلب از بلاگ کیف پول من با ما همراه باشید تا مفهوم، انواع و چالش‌های نتایج تصادفی در بلاکچین و وب 3 را مورد بررسی قرار دهیم.

عدد تصادفی چیست؟



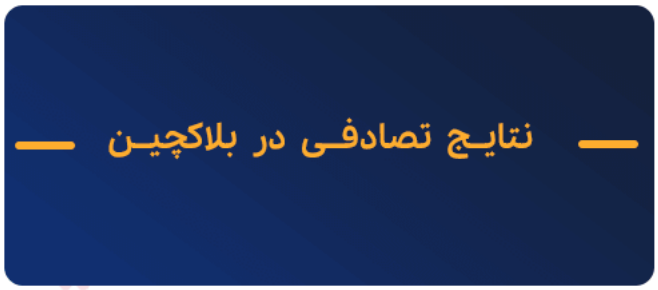
برای آن که به درک درستی از چیستی **نتایج تصادفی در بلاکچین و وب 3** دست پیدا کنید، ابتدا لازم است که با مفهوم عدد تصادفی آشنا شوید. به طور کلی یک عدد تصادفی همان طور که از نام آن پیداست، به عددی اطلاق می‌گردد که به طور تصادفی از یک توزیع مشخص انتخاب شده؛ به نحوی که انتخاب مجموعه‌ای گسترده از اعداد، توزیع زیربنایی را باز تولید می‌نماید. عموما لازم است که چنین نتایجی به شکل مستقل باشند تا میان اعداد متوالی همبستگی ایجاد نگردد. مسئله اعداد و نتایج تصادفی از زمان شکل‌گیری سیستم‌های کامپیوتری همواره مشکل‌ساز بوده‌اند؛ اما وجود مشکلات نتایج تصادفی با قراردادهای هوشمند (Smart Contracts) و شبکه‌های بلاک چینی بیشتر از قبل خواهد شد و همین مسئله بر لزوم آشنایی با این ماهیت در دنیای کریپتوکارنسی می‌افزاید.

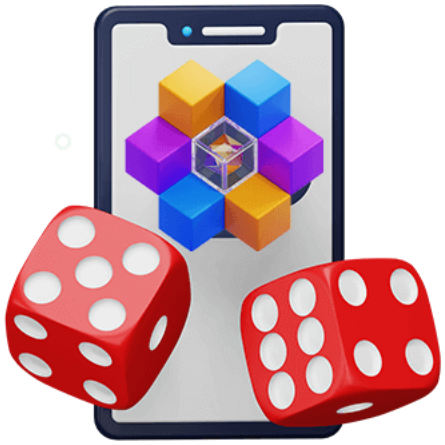
در اصل اگر پروژه رمزارزی شما چندان به اعداد تصادفی وابسته نباشد، در این حالت قادر خواهید بود با هش نمودن برخی از داده‌های عالی، اعداد تصادفی را با سرعت بیشتری در شبکه بلاک چینی تقلید نمائید. حال اگر توکن‌های غیرمثلی و NFTهای خود را توزیع کنید و پروژه شما توجه بخش غالب جامعه را به خود جلب کرده و منابع مالی بیشتری در اختیارتان قرار بگیرد، بی‌شک به دلیل امنیت کم پروژه به سیبل تهاجمات سایبری و حمله هکران تبدیل خواهید شد. یکی از سوالاتی که همواره ذهن کاربران رایانه‌ها و به طور کلی شبکه‌ها دیجیتالی را به خود مشغول ساخته، این است که آیا نتایج تصادفی واقعا تصادفی هستند یا خیر؟! در پاسخ به چنین سوالی باید چند اصل را مورد بررسی قرار دهیم که این اصول به شرح زیر هستند:

- عدم تکرارپذیری: در اصل امکان بازتولید فرآیند تولید نتایج تصادفی وجود نداشته و این حالت صرفا زمانی اتفاق می‌افتد که توالی اصلی حفظ گردد.
- عدم قابلیت پیش‌بینی: تصادفی بودن مستلزم این است که نتایج حاصله غیرقابل تشخیص و پیش‌بینی باشند.
- عدم امکان دستکاری داده‌ها: یکی از ویژگی‌ها و اصول اساسی **نتایج تصادفی در بلاک چین و وب 3** این است که فرآیند تولید این نتایج تصادفی از ایمنی کافی در برابر هرگونه دستکاری احتمالی برخوردار باشند.
- برخورداری از قابلیت اثبات: هر یک از نتایج تصادفی باید به طور کاملا مستقل قابل تائید باشند.
- بی‌طرفانه بودن: منظور از بی‌طرفانه بودن ایجاد شرایط عادلانه است تا هر یک از نتایج تصادفی از شانس برابر و یکسانی برخوردار باشند.

با چنین توضیحاتی روشن می‌شود که جوامع بشری از مدت‌ها پیش به شانس و نتایج تصادفی اعتقاد داشتند و از پرتاب تاس گرفته تا کارت‌خوانی و سایر روش‌های موجود به این نتایج تصادفی دست پیدا می‌کردند که این مسئله با ظهور مبانی ریاضی احتمال و مبانی الگوریتمی و نقش نتایج تصادفی در مطالعات فیزیک کوانتومی، جایگاه ویژه‌تری را به خود اختصاص داده است. امروزه از اعداد تصادفی برای ایجاد الگوریتم‌ها، سیستم‌های رمزنگاری و تراشه‌ها که عموما نقش کلیدی را در تامین امنیت و توسعه فناوری‌های دنیای دیجیتال ایفا می‌کنند، استفاده می‌شود.

نتایج تصادفی در بلاکچین





امروزه **نتایج تصادفی** بیش از هرچیزی در فناوری بلاکچین نمود پیدا کرده‌اند و در واقع روشن شده است که کامپیوترها قادر نیستند به خوبی نشانگر تولیده کننده اعداد تصادفی واقعی باشند و عملا امکان همزیستی آشوب و نظم در یک الگوریتم محال بنظر می‌رسد! مطمئنا یکی از پیشرفت‌های جالب توجه نتایج تصادفی، استفاده از آن‌ها در بلاک چین است و مهم‌ترین اصل رمزنگاری در فناوری بلاکچین چیزی جز ایمن بودن فرآیند تولید نتایج تصادفی نیست. در حال حاضر تابع هش رمزنگاری را می‌توان به عنوان ضروری‌ترین عنصر موجود در تولید کلید خصوصی کیف پول‌های رمزارزی به شمار آورد که در عمل کاربردی جز دشوارتر کردن حدس کلید خصوصی ندارند. برای درک بهتر نتایج تصادفی در بلاکچین و وب 3 به سراغ یک مثال عملی در این حوزه می‌رویم و شبکه بلاک چینی بیت کوین را از این جهت مورد ارزیابی قرار می‌دهیم.

یکی از نوآوری‌های شبکه بلاکچینی بیت کوین که از زمان ظهور خود به آن روی آورده است به استفاده از الگوریتم اجماع اثبات کار (PoW) مربوط می‌شود؛ الگویی که سبب شده تا اعضای شبکه بی‌آن که نیازی به اعتماد به یکدیگر داشته باشند، بر روی تائید تراکنش‌ها به اجماع برسند. منظور از فعالیت «Work» در این الگوریتم اجماع، جستجوی خروجی برای تابع هش (Hash) بوده است و ناگفته نماند که از تابع هش رمزنگاری خاصی به نام SHA-256 در طراحی بیت کوین استفاده شده است. این توابع هش کاملا یک طرفه هستند و عملا نمی‌توان با استفاده از خروجی، داده‌های ورودی را حدس زد که علت اصلی وجود چنین ویژگی به تصادفی بودن خروجی تابع مربوط می‌شود. طبیعتا اگر شبکه بلاک چینی بیت کوین از نتایج تصادفی برای خروجی تابع هش

استفاده نکند، این شبکه به لحاظ امنیتی با مشکلات غیرقابل حلی مواجه شده و یک روزه فرو می‌پاشد!
در شبکه بلاک چینی، جستجوی جواب و خروجی تابع در یک فضای بسیار بزرگ انجام می‌گیرد که نتیجه آن شکل‌گیری روش «Unbounded probabilistic iterative procedure» خواهد بود. ارزیابی تعداد ترکیب‌های کلیدخصوصی امکان‌پذیر در تابع SHA-256 مورد استفاده در پروتکل ارز دیجیتال بیت کوین نشان می‌دهد که تعداد این ترکیب‌ها تقریبا به تعداد تخمینی اتم‌های موجود در دنیا شباهت دارد! وجود چنین سطحی از تصادفی بودن در تابع هش، نشان از قدرت شبکه در تامین امنیت آن دارد.

تصادفی بودن در الگوریتم اثبات سهام (PoS)

در الگوریتم اجماع اثبات سهام (Proof of Stake) نیز از نتایج تصادفی به دلیل برخورداری از زیربنای منصفانه برای توزیع و همچنین غیرقابل پیش‌بینی بودن اعطای مسئولیت به اعتبارسنج‌ها کمک می‌گیرند و کاربرد نتایج تصادفی در بلاکچین و وب 3 صرفا به الگوریتم اجماع اثبات کار منحصر نگردیده است. به بیان بهتر، اگر یک نود مخرب قادر باشد بدون مشکل تصادفی بودن فرآیند انتخاب گره‌ها، شبکه را تحت تاثیر قرار دهد، شانس خود برای انتخاب شدن را افزایش داده و به این شکل امنیت شبکه بلاک چینی را با خطرات قابل توجهی مواجه می‌سازد.

نتایج تصادفی در وب 3

احتمالا تاکنون به هنگام مطالعه و آشنایی با پروژه‌های ان اف تی NFT چندان توجهی به نقش و اهمیت تصادفی بودن فرآیند تعیین نتایج نداشته‌اید؛ حال آن که برای تعیین مکان دارایی‌ها در بازی‌های متاورسی، ضرب NFT، توزیع جوایز و پاداش ها و مواردی از این قبیل در برنامه‌های وب 3 به یک منبع امن تصادفی نیاز داریم تا نتایج را غیرقابل پیش‌بینی کرده و از این طریق انصاف و امنیت را در روند توزیع آیتم‌های مختلف تضمین نماید. وجود تمایل ذاتی به شفافیت و اجرای عدالت در صنعت وب 3 سبب شده تا قفل بسیاری از پروتکل‌های ناموجود در نسخه Web 2 باز شود. طبیعتا اگر چندان آشنایی با روند کار در تعیین نتیجه بازی‌های بلاکچینی نداشته باشید، مطالعه این بخش از نقش **نتایج تصادفی در بلاک چین و وب 3** کمی برای‌تان گنگ خواهد بود. برای درک بهتر اهمیت نتایج تصادفی در وب 3به این مثال توجه کنید:

به عنوان مثال مجموعه NFT میمون‌های کسل (Bored Ape Yacht Club) را در نظر بگیرید. هر یک از توکن‌های غیرمثلی موجود در این مجموعه به دلیل ویژگی‌های منحصربه‌فرد خود دارای ارزش و قیمت متفاوتی هستند. هرچه ویژگی‌های یک میمون کمیاب باشد به همان میزان بر ارزش ذاتی آن افزوده می‌شود.

حال تصور کنید که اگر این مجموعه از فرآیند تصادفی در توزیع توکن‌های خود استفاده نمی‌کرد؛ در این صورت، نتیجه چه می‌شد؟ مسلما در چنین حالتی افراد ذی‌نفوذ در بازار NFT که از سرمایه بیشتری در مقایسه با سایر سرمایه‌گذاران برخوردار هستند، توکن‌های با ویژگی خاص را به قیمتی پایین‌تر خریداری کرده و آن را با قیمت‌های نجومی به فروش می‌رساندند، امری که مطمئنا با سیاست‌های موجود در پروژه‌های NFT متضاد است و در نهایت به شکست مکانیسم‌های اقتصادی پروژه می‌انجامد. طبیعتا دسترسی به یک منبع که از قابلیت ضد دستکاری و غیرقابل پیش‌بینی برخوردار باشد نتیجه‌ایست که استفاده از منابع تصادفی برای پروژه‌های وب 3 به ارمغان آورده است.

نتایج تصادفی؛ تامین کننده امنیت بلاک چین و وب 3

همان طور که عامل **تصادفی بودن نتایج (Randomness)** در طبیعت و دنیای فیزیک کاربردهای زیادی داشته است، ورود این عامل به دنیای کریپتوکارنسی و فضای بلاکچین نیز نتایج بسیار مثبتی را از خود برجای گذاشته است به طوری که شبکه‌های بلاکچینی و پروژه‌های وب 3 جایگاه فعلی خود در جوامع بشری را مدیون وجود نتایج تصادفی هستند که امنیت و عدالت را در آن‌ها تضمین می‌کند. با توجه به اهمیت نتایج تصادفی در بلاکچین و وب 3 ما این مقاله از بلاگ کیف پول من را به بررسی دقیق این مفهوم اختصاص دادیم و همان طور که در مطالب فوق مشاهده کردید، اهمیت استفاده از نتایج تصادفی در بلاکچین و وب 3 به دلایل مختلفی همچون تنوع کاربردهای در بازی‌های بلاکچینی، حاکمیت غیرمتمرکز DAO، پروژه‌های مرتبط با توکن‌های غیرمثلی، رسانه‌های اجتماعی وب 3 و مواردی از این دست، دو چندان شده است.

نقش نتایج تصادفی در تامین امنیت و عدالت شبکه‌های بلاکچینی به قدری است که بدون استفاده از فرآیند تصادفی در خروجی تابع هش در الگوریتم اجماع PoW و انتخاب نودها در الگوریتم PoS، امنیت در شبکه‌های بلاک چینی که دارای ماهیت دیجیتالی هستند، ماهیتی جز شوخی و سرگرمی نخواهد داشت! ناگفته نماند که اگر در ارتباط با مفهوم نتایج تصادفی در بلاکچین و وب 3 سوالی دارید که در مطالب فوق اشاره‌ای به پاسخ آن نشده است، می‌توانید سوال خود را در بخش نظرات مطرح کنید تا کارشناسان مادر اسرع وقت به سوال شما پاسخ دهند.