

کوبین ایران

مقدمه‌ای بر فناوری (DAG) Directed Acyclic Graph

فهرست مطالب

۱.....	مقدمه‌ای بر فناوری Directed Acyclic Graph (DAG)
۱.....	فناوری گراف جهت‌دار غیرمدور
۳.....	مزایای فناوری گراف جهت‌دار غیرمدور
۳.....	معایب فناوری گراف جهت‌دار غیرمدور
۴.....	تعریف گراف جهت‌دار غیرمدور
۶.....	نمونه‌های عملی از به کارگیری فناوری گراف جهت‌دار غیرمدور
۶.....	IOTA
۶.....	Byteball
۷.....	Railblocks
۷.....	Fantom Foundation
۸.....	منابع

مقدمه‌ای بر فناوری (DAG) Directed Acyclic Graph

فناوری گراف جهت‌دار غیرمدور^۱ (DAG) یکی از چهار فناوری شناخته‌شده برای دفتر کل توزیع شده یعنی بلاک‌چین، Hashgraph، DAG و Holochain می‌باشد که به جای استخراج، از تأیید تراکنش‌های دیگر برای ثبت تراکنش استفاده می‌کند. این فناوری با توجه به بازار رقابتی دفتر کل توزیع شده^۲ (DLT) و پتانسیل بالایی که دارد می‌تواند آینده دنیای رمز ارزها را رقم بزند. فناوری گراف جهت‌دار غیرمدور با توجه به استفاده از ساختار داده گرافی می‌تواند مقیاس‌پذیری و سرعت انجام تراکنش‌ها را به طرز چشم‌گیری افزایش دهد. این فناوری که از آن به عنوان نسل سوم بلاک‌چین نیز یاد می‌شود تحول عظیمی در صنایع نیازمند پرداخت‌های خرد به ویژه حوزه اینترنت اشیاء ایجاد کرده است.

فناوری گراف جهت‌دار غیرمدور

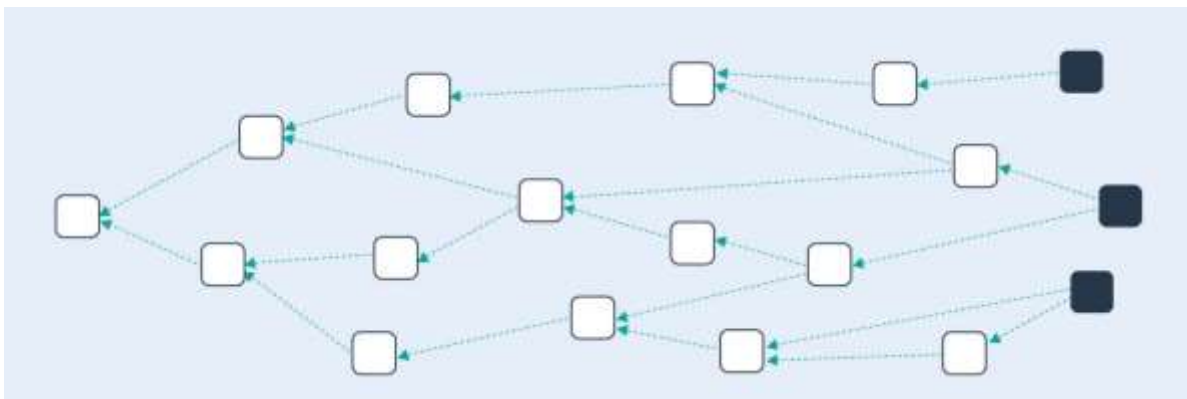
این فناوری بر اساس تئوری گراف‌ها عمل می‌کند. DAG گرافی است که هیچ دوری در آن وجود ندارد و تمامی یال‌های آن یک طرفه هستند. در این نوع گراف، با شروع پیمایش از گره امکان بازگشت به آن وجود ندارد. این فناوری جایگزین ارزشمندی برای رویکرد سنتی دفتر کل توزیع شده ارائه می‌دهد که با کاهش هزینه تراکنش، بهبود شفافیت و افزایش کارایی همراه است. DAG یک پلتفرم پایدار در اختیار شرکت‌ها قرار می‌دهد تا تمامیت تراکنش‌ها و دارایی‌های دیجیتال خود را حفظ نمایند [۱].

DAG نیز همانند بلاک‌چین از یک شبکه با تعدادی از گره‌های مختلف تشکیل شده است که تراکنش‌ها را تأیید می‌کنند. هر تراکنش جدید شبکه نیازمند تأیید حداقل دو تراکنش قبلی است تا با موفقیت ثبت شود. با ارسال تراکنش‌های بیشتر، تراکنش‌های بیشتری نیز تأیید شده و وارد شبکه می‌شوند که این امر منجر به توزیع وبی از تراکنش‌های دوبار تأیید شده^۳ خواهد شد [۲].

^۱ Directed Acyclic Graph (DAG)

^۲ Distributed Ledger Technology (DLT)

^۳ Doubly-Confirmed

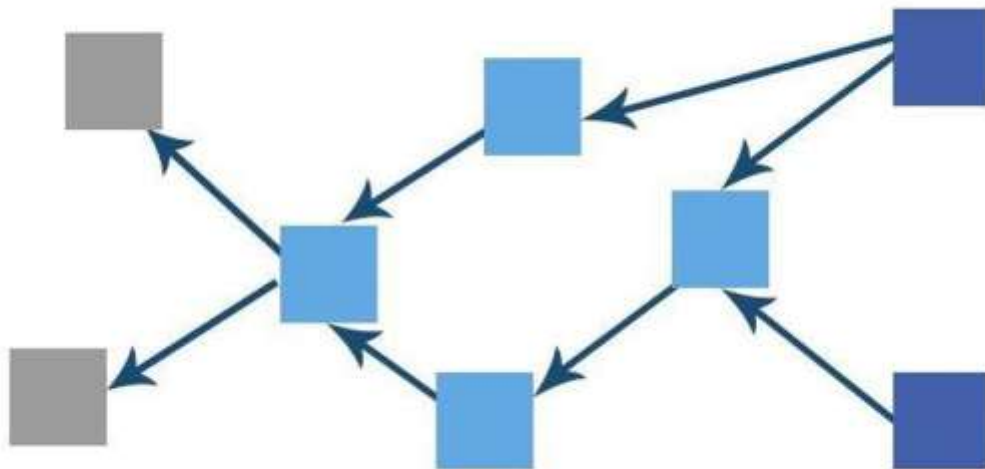


بلاک‌چین بر اساس ساختار داده‌ای لیست پیوندی پایه‌ریزی شده است. هر ورودی جدید در شبکه بلاک‌چین پس از آخرین بلوک قرار می‌گیرد و دارای یک ارجاع به بلوک ماقبل خود است. بدین ترتیب یک دنباله خطی از رویدادهای دیجیتال ایجاد می‌شود که زنجیره نام دارد. بلاک‌چین امکان رهگیری تمامی رکوردهای ذخیره شده را فراهم می‌نماید ولی ساختار ترتیبی، توان عملیاتی شبکه را به شدت کاهش می‌دهد. تأخیر بالا و مقیاس‌پذیری کم از دیگر چالش‌های عمده پیش روی بلاک‌چین به شمار می‌روند [۳، ۴].

ساختار داده‌ای گراف جهت‌دار غیرمدور مانند یک نمودار جریان است که همه نقاط در یک جهت هدایت می‌شوند. ساختار DAG همانند ساختار داده‌ای درخت است که هر گره دارای زیرگره‌هایی متصل به آن است. این رویکرد غیرخطی امکان رشد شبکه و سرعت بالای تصدیق تراکنش‌ها را تضمین می‌نماید. علاوه بر این، گراف جهت‌دار غیرمدور با استفاده از مجوزهای triple-attribute و استانداردهای معنایی واحد^۱ می‌تواند قابل اعتماد شده و برای همکاری متقابل در سطح جهانی مورد استفاده قرار گیرد. فناوری گراف جهت‌دار غیرمدور با هدف کاهش تأخیر مورد نیاز در فرآیند اعتبارسنجی تراکنش‌های بلاک‌چین، توسعه داده شده است. تراکنش‌های جدید در ساختار DAG تنها نیازمند تصدیق دو تراکنش دیگر هستند تا زنجیره اعتماد در شبکه تکمیل شود. این فناوری معمولاً در مورد مسائل مربوط به پردازش داده، زمان‌بندی، یافتن بهترین مسیر در ناوبری و فشرده‌سازی داده به کار می‌رود [۴، ۵].

NXT اولین جامعه‌ای بود که ایده تغییر ساختار ذخیره‌سازی زنجیره‌ای را به گراف جهت‌دار غیرمدوری از بلوک‌ها تغییر داد. بر این اساس، اگر زمان استخراج بدون تغییر باقی بماند ذخیره‌سازی می‌تواند با X بلوک در شبکه به اندازه X بار در آن واحد بیشتر شود.

^۱ Uniform Semantic Standards



مزایای فناوری گراف جهت‌دار غیرمدور

از مهم‌ترین مزایای گراف جهت‌دار غیرمدور می‌توان به موارد زیر اشاره کرد [۶].

- گراف جهت‌دار غیرمدور از مقیاس‌پذیری خوبی برخوردار است که به معنای سرعت بالای تراکنش‌های آن می‌باشد. گره‌ها تنها اعتبارسنج‌ها و تأییدکننده‌های تراکنش‌ها هستند و برای تأیید تراکنش نیازی به تشکیل بلوک نیست. اطلاعات در داخل تراکنش‌ها قرار می‌گیرند که به سرعت بسیار بالای آن منجر می‌شود. از نظر تئوری، امکان انجام میلیون‌ها تراکنش در این روش وجود دارد که یک خبر خوب برای جامعه رمز ارزها به شمار می‌رود.
- تمامی تراکنش‌های DAG توسط گره‌ها تأیید می‌شوند که این امر قابلیت اطمینان بالای این ساختار را به همراه دارد.
- مصرف انرژی این روش نسبت به دیگر مکانیسم‌های اجماع مانند گواه اثبات کار^۱ (POW) کمتر است که به معنای غیرمتمرکزسازی بیشتر است.
- الگوریتم DAG به دلیل کمیسیون نزدیک به صفر آن برای سیستم‌های پرداخت خرد ایده‌آل است.

معایب فناوری گراف جهت‌دار غیرمدور

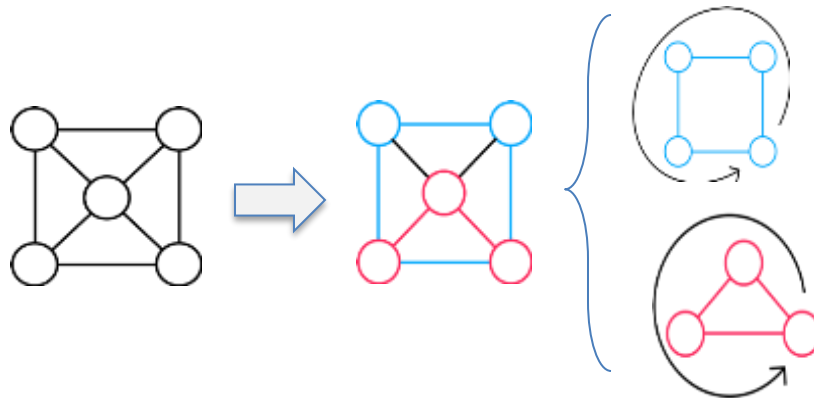
گراف جهت‌دار غیرمدور با وجود تمام مزایای آن نوش‌دارویی برای دنیای رمز ارزها نیست و محدودیت‌های مخصوص به خود را دارد [۶].

^۱ Proof Of Work (POW)

- این روش با وجود مقیاس پذیری بسیار بالا نسبت به سیستم‌های کنونی نمی‌تواند انتظارات سیستم‌های آینده را برآورده نماید.
- هیچ اطلاعاتی در مورد محافظت از الگوریتم و ساختار گراف جهت‌دار غیرمدور در برابر خرابی‌های سیستمی ارائه نشده است.

تعریف گراف جهت‌دار غیرمدور

گراف مدور^۱ نوعی گراف یا شبکه‌ای از گره‌های متصل است که اطلاعات می‌توانند در مسیرهای [یال‌های] مختلف موجود از یک گره به گره دیگر منتقل شوند و با گذر از گره‌های میانی دوباره به گره اصلی بازگردند. اطلاعات باید تنها یک بار از گره‌های میانی موجود در مسیر عبور کنند تا یک گراف مدور تشکیل شود. در شکل زیر، گراف اصلی و بخش‌های مشتق شده از آن که با رنگ آبی و قرمز نشان داده شده‌اند نمونه‌ای از گراف‌های مدور می‌باشند [۷].



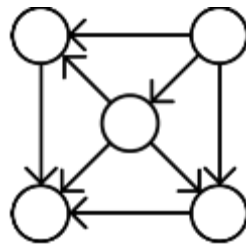
گراف‌های غیرمدور، گراف‌های هستند که هیچ دوری در آن‌ها وجود نداشته باشد. در شکل زیر نمونه‌ای از گراف‌های غیرمدور آورده شده است. اطلاعات در این گراف‌ها هیچ راهی برای بازگشت به گره مبدأ ندارند مگر اینکه از یک مسیر یا یک گره دوبار عبور کنند.



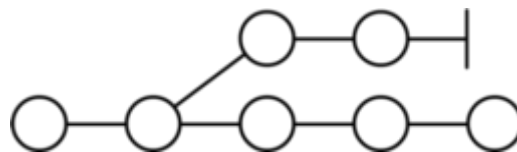
اگر برای هر یک از مسیرها یک جهت حرکتی یک طرفه تعیین شود و بین هرکدام از گره‌ها تنها یک مسیر وجود داشته باشد گراف جهت‌دار غیرمدور تشکیل می‌شود. این بدین معنی است که با شروع از یک گره نمی‌توان از تمامی گره‌های گراف عبور کرد. حرکت در گراف جهت‌دار تنها در یک مسیر امکان پذیر است. گراف، بیانگر یک مرتب‌سازی توپولوژیک است که هر گره در یک نظم خاص قرار دارد. ساختار DAG شامل رئوسی (گره) است که توسط یال‌ها

^۱ Cyclic Graph

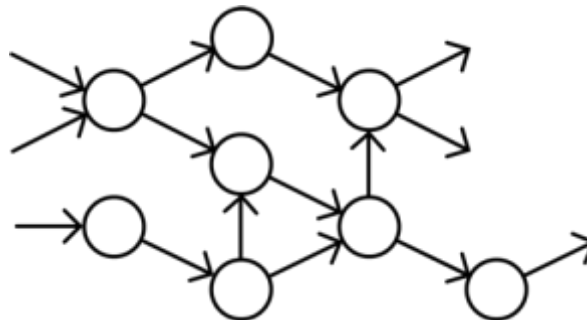
(مسیرها) به یکدیگر متصل شده‌اند. الگوریتم اصلی DAG مرتب‌سازی توپولوژیکی نامیده می‌شود و این بدان معنی است که هر یال از آخرین گره موجود به گره جدید وصل می‌شود [۶].



منطق عملکرد گراف جهت‌دار غیرمدور به بلاک‌چین بسیار نزدیک است به ویژه هنگامی که یک زنجیره از بلوک‌ها وجود داشته باشد و هر بلوک جدید دارای یک ارجاع به بلوک قبلی باشد. زنجیره‌های منشعب‌شده^۱ از بزرگ‌ترین مشکلات این ساختارها می‌باشند که در صورت استخراج همزمان دو بلوک یا حمله ۵۱ درصد ایجاد می‌شوند. بلاک‌چین‌ها برای حفظ اعتبار زنجیره اصلی از یک دوره زمانی دلخواه بین استخراج بلوک‌ها استفاده می‌کنند که شبکه، فرصت کافی برای شناسایی زنجیره درست و تحکیم شبکه اصلی را داشته باشد. این زمان انتظار به عنوان **زمان [تولید] بلوک**^۲ شناخته می‌شود و امکان حذف شاخه‌های مخرب یا کوتاه‌تر را فراهم می‌نماید [۷].



در طرف مقابل، گراف جهت‌دار غیرمدور (DAG) اجازه می‌دهد تا چندین زنجیره از بلوک‌ها به طور همزمان وجود داشته و با یکدیگر در ارتباط باشند. با این حال، نباید هر مسیری به گره والد (گره مبدأ) وجود داشته باشد. اگر اطلاعات در مسیرهای یک طرفه به درستی هدایت شوند گره‌ها می‌توانند به صورت موازی ایجاد شوند.



روش DAG گزینه‌های جدیدی را برای تأیید اعتبار یک بلوک ایجاد می‌کند که نیازی به زمان بلوک ندارند. همچنین این روش مقدار کار تلف شده برای تولید شاخه‌ها و زنجیره‌های بی‌استفاده^۳ را به شدت کاهش می‌دهد؛

^۱ Branched Chains

^۲ Block Time

^۳ Orphan-Chains

بنابراین، پتانسیل بی‌سابقه‌ای برای دستیابی به جریان اطلاعات سریع و مقیاس‌پذیر در یک شبکه کاملاً غیرمتمرکز فراهم می‌شود [۷].

نمونه‌های عملی از به کارگیری فناوری گراف جهت‌دار غیرمدور

کوین‌های متعددی بر اساس فناوری گراف جهت‌دار غیرمدور توسعه داده شده است. IOTA از معروف‌ترین کوین‌های توسعه‌یافته با این روش است که در ادامه به همراه نمونه‌های دیگر معرفی می‌شوند [۳، ۶].

IOTA

IOTA یکی از شناخته‌شده‌ترین کوین‌هایی است که از DAG استفاده می‌کند و اولین پروژه‌ای است که در زمان صحبت درمورد گراف جهت‌دار غیرمدور باید به آن اشاره کرد. IOTA معرف نسل جدیدی از رمز ارز است که مفهوم هزینه استخراج را به طور کامل از بین برد. در حال حاضر، حجم بازار این رمز ارز بیش از یک میلیارد دلار است. نام این رمز ارز از اینترنت اشیاء^۱ گرفته شده است و هدف اصلی آن ایجاد اکوسیستمی برای پرداخت‌های خرد است؛ چراکه در آینده نزدیک تمامی دستگاه‌ها به اینترنت متصل خواهند شد و تعداد تراکنش‌ها به شدت افزایش خواهد یافت. امکان انجام میلیاردها تراکنش با کمیسیون بسیار پایین از نقاط قوت IOTA برای اکوسیستم جدید خواهد بود. همکاری IOTA و DAG منجر به تولد Tangle شده است. Tangle این فناوری را در ابعاد جدیدی در IOTA گسترش داده است و بر اساس وایت‌پیپر آن بیشتر به گراف جهت‌دار غیرمدور سه بعدی (3D) شباهت پیدا است. هر تراکنش Tangle باید دو تا از تراکنش‌های پیشین را تأیید کند که به طور تصادفی توسط شبکه انتخاب می‌شوند. همچنین اتصال الگوریتم این رمز ارز با DAG امکان ایجاد بخش‌های آفلاین شبکه را نیز فراهم می‌نماید. هر کدام از خوشه‌های آفلاین با اتصال به اینترنت به بخشی از بلاک‌چین عمومی تبدیل می‌شوند.

Byteball

پروژه رمز ارز Byteball از مزیت‌های ساختار داده‌ای DAG به منظور ایجاد اکوسیستم قراردادهای هوشمند برای پرداخت‌های سریع و ذخیره‌سازی داده‌های مالی مانند ارزها، املاک، بدهی‌ها، سهام و ... استفاده می‌کند. این پروژه‌ی غیربلاک‌چینی که بر اساس ساختار گراف جهت‌دار غیرمدور پایه‌ریزی شده است با کیف پول‌های ساده و کاربرپسند در دسترس کاربران قرار دارد. این پروژه دارای ۱۲ شاهد یا نود اصلی مورد اعتماد است که تمامی تراکنش‌های شبکه را تصدیق می‌نمایند.

Byteball در زمینه قراردادهای هوشمند هم‌تا به هم‌تا از کارایی بالایی برخوردار است. کاربران Byteball می‌توانند از پرداخت‌های هوشمند مشروط خالی از ریسک استفاده کنند. تنها کاری که کاربران باید انجام دهند این است که

^۱ Internet of Things

شرایط مربوط به دریافت پول توسط دریافت‌کننده وجه را تعیین نمایند. اگر شرط تعیین‌شده برآورده نشده باشد پول به صورت خودکار به حساب پرداخت‌کننده بازگردانده می‌شود. به عنوان مثال، Byteball به بیمه‌های هم‌تا به هم‌تا اجازه می‌دهد تا در پلتفرم مبتنی بر قراردادهای هوشمند، خریداری شده و به فروش برسند.

Railblocks

Railblocks یک ابزار لحظه‌ای، بدون هزینه و بی‌نهایت مقیاس‌پذیر مبتنی بر ساختار داده‌ای DAG برای انجام تراکنش است. شبکه Railblocks فاقد ماینر است و یک دفتر کل عمومی غیرقابل اشتراک‌گذاری به شمار می‌رود. هرکس بلوک اختصاصی خود را دارد که خودش آن را تأیید می‌کند. این روش پیاده‌سازی گواه اثبات سهام، Balance of vote نام دارد. Railblocks یک پروژه متن باز است و فروش اولیه سکه برای آن انجام نشده است؛ با این وجود، شبکه و کیف پول اختصاصی آن در دسترس کاربران قرار دارد. این پروژه از الگوریتم‌های SHA3/Blake2 و منحنی بیضوی ED25519 استفاده می‌کند [۸].

Fantom Foundation

Fantom ادعا می‌کند که اولین قراردادهای هوشمند مبتنی بر DAG را توسعه داده است. این پروژه از معماری DAG در فناوری دفتر کل توزیع شده استفاده کرده است. Fantom چالش‌های مربوط به سرعت و مقیاس‌پذیری قراردادهای هوشمند مبتنی بر بلاک‌چین امروزی را حل‌وفصل نموده است و می‌تواند تا ۳۰۰۰۰۰ تراکنش در ثانیه با هزینه‌ای کمتر از ۱ سنت به ازای هر تراکنش ارائه نماید. تراکنش‌ها به صورت ناهمگام و تأیید لحظه‌ای انجام می‌شوند که به مقیاس‌پذیری هرچه بیشتر این پروژه منجر شده است. Fantom تأکید ویژه‌ای بر روی اعتماد دارد و کاربردهای فراوانی در صنایع غذایی و اینترنت اشیا برای آن تعریف شده است. این پروژه از نام Opera Chain برای گراف جهت‌دار غیرمدور خود استفاده کرده است که از تأیید افراد، مدیریت community، سرویس‌های مالی و ... پشتیبانی می‌کند. Fantom با استفاده از ماشین مجازی اختصاصی خود، امکان اجرای مؤثر قراردادهای هوشمند در سیستم عامل‌های مختلف را فراهم می‌کند.

- [١] Kotilevets, ID; Ivanova, IA; Romanov, IO; Magomedov, SG; Nikonov, VV; Pavelev, SA“ ,Implementation of directed acyclic graph in blockchain network to improve security and speed of transactions ”,*IFAC-PapersOnLine* , جلد ٥١, شماره ٣٠, pp. 693--696, 2018 .
- [٢] J. Evans“ ,Breaking the Chain – Directed Acyclic Graph“) DAG (“challenges Blockchain’s dominance ”,Hassans . ,Available: [http://www.gibraltarlaw.com/directed-acyclic-graph-vs-blockchain./](http://www.gibraltarlaw.com/directed-acyclic-graph-vs-blockchain/)
- [٣] I. Kohut“ ,Cryptocurrencies Without Blockchain? Learn More About Directed Acyclic Graphs (DAG) ”,Perfectial . ,Available: [https://perfectial.com/blog/dag-vs-blockchain./](https://perfectial.com/blog/dag-vs-blockchain/)
- [٤] J. Aasman“ ,Going Beyond Blockchain with Directed Acyclic Graphs (DAG) ”, Cryptoslate . ,Available: [https://cryptoslate.com/beyond-blockchain-directed-acyclic-graphs-dag./](https://cryptoslate.com/beyond-blockchain-directed-acyclic-graphs-dag/)
- [٥] S. Lee“ ,Explaining Directed Acyclic Graph (DAG), The Real Blockchain 3.0 ”,Forbes . , Available: <https://www.forbes.com/sites/shermanlee/2018/01/22/explaining-directed-acyclic-graph-dag-the-real-blockchain-3-0/#71785ea4180b>.
- [٦] BitcoinWiki“ ,Directed acyclic graphs (DAGs) ”,BitcoinWiki . ,Available: [https://en.bitcoinwiki.org/wiki/Directed_acyclic_graphs_\(DAGs.\)](https://en.bitcoinwiki.org/wiki/Directed_acyclic_graphs_(DAGs.))
- [٧] Fantom Foundation“ ,An Introduction to DAGs and How They Differ From Blockchains ”,Fantom Foundation . ,Available: <https://medium.com/fantomfoundation/an-introduction-to-dags-and-how-they-differ-from-blockchains-a6f703462090>.
- [٨] S. Muhammad“ ,DAG (Directed Acyclic Graph) - A competitor to Blockchain ”,! LinkedIn . ,Available: [https://www.linkedin.com/pulse/dag-directed-acyclic-graph-competitor-blockchain-shakil-muhammad./](https://www.linkedin.com/pulse/dag-directed-acyclic-graph-competitor-blockchain-shakil-muhammad/)



کوین ایران بزرگ‌ترین پایگاه خبری فارسی زبان در حوزه فناوری بلاک‌چین، ارزهای رمزنگاری شده و پلتفرم‌های مرتبط با بلاکچین است. این وب سایت در سال ۱۳۹۲ توسط بابک جلیوند و آرش محبوب، با هدف اطلاع‌رسانی، آموزش و مشاوره به جامعه فارسی زبان علاقه‌مند به رمز ارزها راه‌اندازی 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.

<https://coiniran.com>

نویسنده: تورج اکبری

آدرس ایمیل: Turaj.akbari68@yahoo.com

