کوین ایران

اجماع مقیاس‌پذیر برای شبکه‌های خصوصی با الگوریتم

Istanbul Byzantine Fault Tolerant (IBFT)

فهرست مطالب

اجماع مقیاس‌پذیر برای شبکه‌های خصوصی با الگوریتم IBFT

الگوریتم‌های اجماع یکی از اصلی‌ترین نوآوری‌های بلاک‌چین و در عین حال یکی از گیج‌کننده‌ترین آن‌ها به شمار می‌رود. ساتوشی ناکاموتو نسخه‌ای از اثبات کار[۱] (PoW) را ایجاد کرد که به عنوان ابزاری برای تأمین همزمان امنیت و اعتبارسنجی تراکنش‌های بیت‌کوین پیاده‌سازی شده بود. جامعه بلاک‌چین در ادامه، الگوریتم‌های اجماع دیگری مانند اثبات سهام[۲] (PoS)، اثبات اقتدار[۳] (PoA)، تحمل خطای بیزانس عملی[۴] (PBFT)، تحمل خطای بیزانس استانبول[۵] (IBFT) و بسیاری دیگر از الگوریتم‌ها را ایجاد کرد که به منظور دستیابی به اجماع در سیستم‌های توزیع شده و ایجاد منبع واحد اعتماد طراحی شده بودند. IBFT نوعی راه‌حل تحمل خطای بیزانس[۶] است که نیاز به زیرساخت اثبات کار را با تضمین قطعیت آنی تراکنش‌ها کاهش داده است. قطعیت به این معنی است که پس از اضافه شدن یک تراکنش به بلوک و قرارگیری آن در بلاک‌چین دیگر امکان ابطال آن وجود ندارد. IBFT یک شبکه تک سطحی است که امکان فورک و زنجیره جانبی ندارد. این مکانیسم اجماع در زنجیره‌های خصوصی با استخرهای اعتبارسنجی قابل اعتماد و پاسخگو از کارایی بالایی برخوردار است. تحمل خطای بیزانس استانبول یک راه‌حل ایده‌آل برای شبکه‌هایی با نرخ قابل پیش‌بینی تراکنش می‌باشد.

الگوریتم‌های اجماع همواره در تلاش هستند تا مصالحه‌ای مابین کارایی و امنیت تراکنش ایجاد کنند. کارایی در شبکه بلاک‌چین معمولاً بر اساس توان انجام تراکنش سنجیده می‌شود؛ به عنوان مثال، شبکه اصلی اتریوم که از اثبات کار استفاده می‌کند از امنیت بسیار بالایی برخوردار است ولی کارایی آن قابل قبول نیست. در طرف مقابل، بلاک‌چین‌های خصوصی که از مکانیسم اثبات اقتدار استفاده می‌کنند از کارایی بالایی برخوردارند ولی امنیت آن‌ها پایین است. امنیت در شبکه بلاک‌چین برای بیان مقاومت شبکه در برابر بازیگران مخرب و ارائه عملکرد از پیش تعیین شده مورد استفاده قرار می‌گیرد. الگوریتم‌های پیشرفته اثبات اقتدار مانند IBTF در بین این دو طیف قرار می‌گیرند و همزمان با افزایش کارایی می‌توانند در مقابل بازیگران مخرب نیز مقاومت کنند [۱].

---

[۱] Proof of Work (PoW)

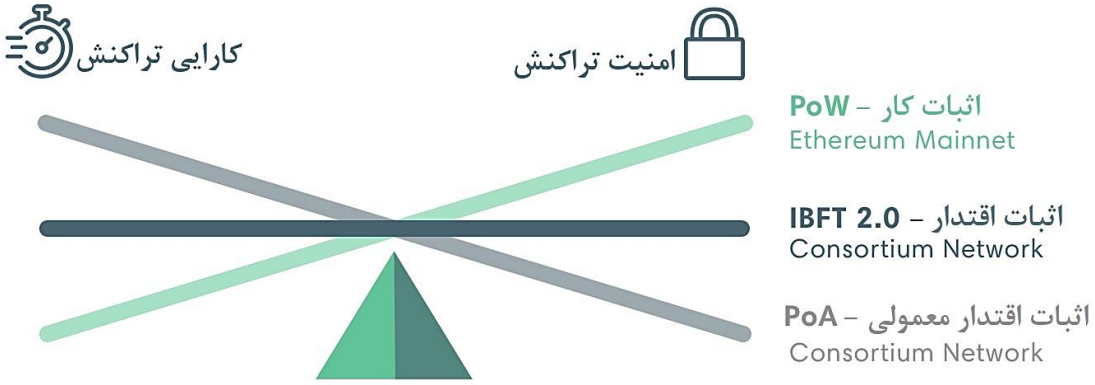
[۲] Proof of Stake (PoS)

[۳] Proof of Authority (PoA)

[۴] Practical Byzantine Fault Tolerant (PBFT)

[۵] Istanbul Byzantine Fault Tolerant (IBFT)

[۶] Byzantine Fault Tolerance (BFT)



تحمل خطای بیزانس استانبول (IBFT)

تحمل خطای بیزانس استانبول (IBFT) مکانیسم اجماعی است که به عنوان جایگزینی برای گواه اثبات کار در شبکه اتریوم معرفی شده است. IBFT همانند الگوریتم‌های دیگر از وجود ترتیب واحد و مورد توافق از تراکنش‌ها در بلاک‌چین اطمینان حاصل می‌کند. تحمل خطای بیزانس استانبول برای استفاده در بلاک‌چین‌های خصوصی و کنسرسیوم توسعه داده شده است و کاربردی در بلاک‌چین‌های عمومی نخواهد داشت. این الگوریتم مزایای دیگری مانند قطعیت تسویه حساب را نیز برای سازمان‌ها به همراه دارد [۱].

Istanbul BFT یک پیاده‌سازی اصلاح شده از الگوریتم تحمل خطای بیزانس عملی می‌باشد. مهم‌ترین تفاوت این الگوریتم با دیگر الگوریتم‌های تحمل‌پذیر خطا در این است که به جای اعتماد کورکورانه به رهبران شبکه در ایجاد هر بلوک، چندین مرحله رأی‌گیری میان گروهی از اعتبارسنج‌ها انجام می‌دهد تا به توافق متقابل دست یابد. توافق متقابل به عنوان مجموعه‌ای از امضاها در محتوای بلوک ثبت می‌شود. یک اعتبارسنج هرگز رهبر یا پیشنهاد دهنده بلوک را صادق یا درست فرض نمی‌کند و مانند مکانیسم‌های اجماعِ محیط‌های فاقد اعتماد عمل می‌کند [۲].

تحمل خطای بیزانس به معنای شبکه‌ای است که می‌تواند با وجود گره‌های[۱] متقلب نیز به عملیات صحیح خود ادامه دهد. گره‌های متقلب تلاش می‌کنند که بلوک‌های غیرمعتبر را پیشنهاد دهند یا بلوک‌های حافظ منافع برخی از اعضای شبکه را تأیید کنند. پیاده‌سازی PBFT که IBFT نیز بر مبنای آن پیاده‌سازی شده می‌تواند وجود f گره متقلب در شبکه‌ای شامل 3f+1 گره را تحمل کند. این به معنای توانایی تحمل خطای عمدی حدود ۳۰ درصد از گره‌های شبکه می‌باشد.

[۱] Nodes

ویژگی گره‌ها از نقش تعیین‌کننده‌ای در انتخاب IBFT برخوردار است. اگر گره‌ها متعلق به گروهی مانند اصلی‌ترین رقبای سازمان باشد که نمی‌توان همیشه به آن اعتماد کرد یا معیارهای امنیتی به درستی در آن‌ها پیاده‌سازی نشده باشد باید به سمت استفاده از IBTF حرکت کرد. شبکه‌ای که از IBTF استفاده می‌کند صرف نظر از وجود تراکنش‌های در انتظار، همیشه بلوک‌ها را در فاصله‌های زمانی ثابت تولید می‌کند. بنابراین اگر سرعت تولید تراکنش پایین باشد بلوک‌های زیادی بدون وجود تراکنش ساخته خواهند شد. بلوک‌های تولیدشده از طریق به کارگیری اعتبارسنج‌های حاضر در رأی‌گیری و جمع‌آوری امضا از پیشنهاددهنده به شدت در مقابل دستکاری محافظت می‌شوند. بازنویسی محتوای بلوک بدون دسترسی به کلیه کلیدهای خصوصی امضای پیشنهاددهندگان و گره‌های اعتبارسنج غیرممکن است. این روش تضمینی برای تغییرناپذیری بلاک‌چین حاصل‌شده خواهد بود.

لیست اعتبارسنج‌های حاضر در رأی‌گیری با توجه به درخواست اعتبارسنج‌ها می‌تواند تغییر کند. این تغییرات با رأی اعضا انجام می‌شود و می‌تواند اعتبارسنج‌های جدیدی را به لیست اضافه کرده یا از آن حذف نماید.

- برای اضافه کردن اعتبارسنج جدید باید حداقل ۶۶ درصد از اعتبارسنج‌های موجود یک تابع مشخص با نام istanbul.propose(new_node_address, true); را فراخوانی کنند.
- برای اخراج کردن اعتبارسنج موجود باید حداقل ۶۶ درصد از اعتبارسنج‌های موجود یک تابع مشخص با نام istanbul.propose(new_node_address, false); را فراخوانی کنند.

مزیت‌های تحمل خطای بیزانس استانبول (IBFT)

الگوریتم اثبات کار از نظر سخت‌افزاری و برق بسیار پرهزینه است. این هزینه‌ها به صورت عمدی و برای جلوگیری از تصرف آسان شبکه در نظر گرفته شده است. الگوریتم اثبات کار برای شبکه‌های کاملاً غیرمتمرکز با امکان مشارکت همگانی بسیار مناسب است. با این حال، گره‌های موجود در زنجیره‌های خصوصی/ کنسرسیومی که توسط شرکت‌ها مورد استفاده قرار می‌گیرد نسبت به زنجیره‌های عمومی قابل اعتمادترند. همچنین ممکن است مکانیسم اجماع اثبات کار (PoW) برای استفاده در تمامی شبکه‌ها بسیار سنگین باشد و مکانیسم‌های دیگر اعتماد کافی برای اجرا در سیستم توزیع‌شده را فراهم نمایند. به همین ترتیب، اثبات سهام به دلیل استفاده از Gas کارایی چندانی در شبکه‌های مجوزدار نخواهد داشت. با توجه به این مسائل، اثبات اقتدار (PoA) به عنوان بهترین راه‌حل ممکن برای شبکه‌های خصوصی ظهور کرد. این الگوریتم از سیستمی استفاده می‌کند که بر اساس آن گره‌های شبکه می‌توانند امتیاز تولید بلوک‌های جدید زنجیره را با روش Round-Robin یا روش‌های مشابه دیگر تخصیص دهند. تحمل خطای بیزانس استانبول (IBFT) یکی از مکانیسم‌های مبتنی بر اثبات اقتدار است که مزیت‌های زیر را به همراه دارد [۳, ۴].

- **قطعیت آنی بلوک:** در شـــبکه مبتنی بر IBFT امکان وجود فورک و انشـــعاب زنجیره وجود ندارد؛ بنابراین در هیچ شرایطی بازگشت تراکنش امکان‌پذیر نیست.

- **کاهش زمان بین بلوک‌ها:** مدت زمان تولید و اعتبارسنجی بلوک در قیاس اثبات سهام به شدت کاهش یافته است. کاهش زمان تولید بلوک به افزایش توان عملیاتی شبکه منجر شده است.
- **یکپارچگی بالای داده و تحمل‌پذیری خطا:** IBTF از گروهی از اعتبارسنج‌ها برای اطمینان از یکپارچگی بلوکِ پیشنهاد شده استفاده می‌کند. اکثریت قالب (حدود ۶۶ درصد) این اعتبارسنج‌ها باید قبل از اضافه شدن بلوک به زنجیره، آن را امضا کنند. رهبری گروه اعتبار سنج هم به صورت دوره‌ای عوض می‌شود تا از تأثیر طولانی مدت گره‌های مشکوک بر زنجیره جلوگیری نماید.
- **انعطاف‌پذیری عملیاتی:** گروه اعتبارسنج‌ها در صورت نیاز می‌تواند تغییر کند تا اطمینان حاصل شود که تنها گره‌های کاملاً مورد اعتماد در گروه عضویت دارند.

تاریخچه مختصر تحمل خطای بیزانس استانبول

IBFT برای اولین بار توسط Amis Technologies در Geth پیاده‌سازی شد و پس از آن در Quorum مورد استفاده قرار گرفت. Quorum اولین مشتری اتریوم سازمانی بود که سه الگوریتم اجماع مختلف را به منظور دستیابی به یک راه‌حل قابل قبول برای بلاک‌چین‌های سازمانی پیاده‌سازی کرد. این الگوریتم‌ها که با نام‌های RAFT، Clique و IBTF 1.0 شناخته می‌شوند هر کدام برای استفاده در یک مورد کاربردی خاص توسعه داده شدند. IBFT در Quorum نشان داد که می‌تواند یک الگوریتم اجماع جذاب برای شبکه‌های مجوزدار سازمانی نیازمند تحمل خطای بیزانس (BFT) و قطعیت تراکنش باشد.

حوزه‌های کاربردی IBFT 1.0

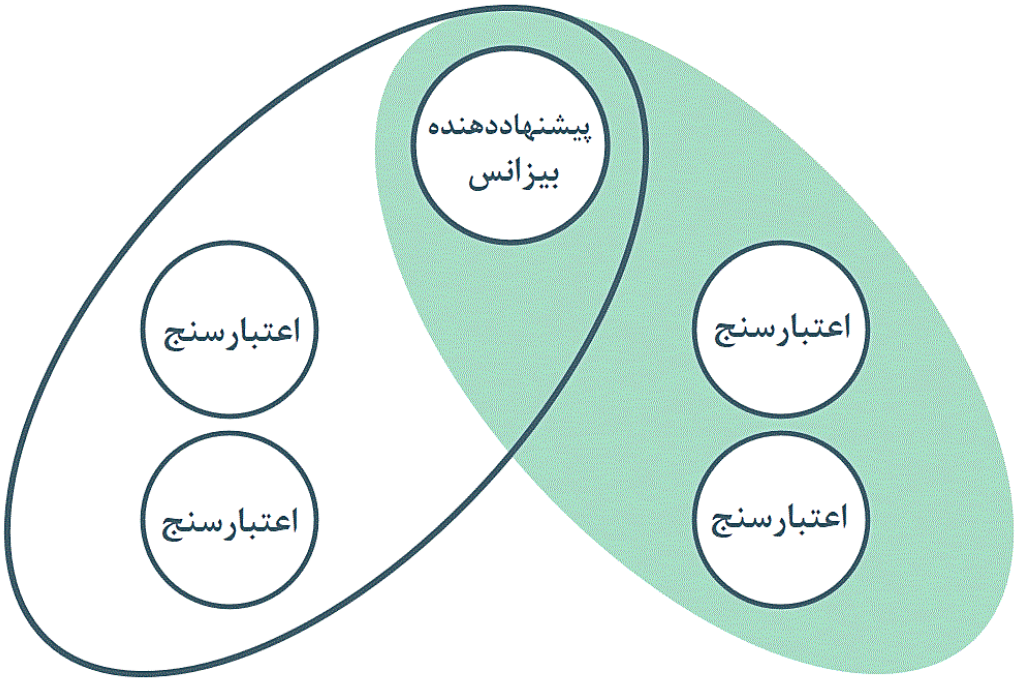
الگوریتم اجماع بلاک‌چین همواره باید از ایمنی[۱] و ادامه حیات[۲] آن اطمینان حاصل کند. ایمنی یعنی هیچ اتفاق بدی رخ نخواهد افتاد. وقتی ایمنی در یک الگوریتم اجماع مانند IBTF با قطعیت آنی مورد استفاده قرار می‌گیرد بدین معنی است که هیچ دو بلوک معتبر و متفاوت با ارتفاع یکسان نمی‌توانند تولید شوند. قطعیت یکی ویژگی ایمنی است. ادامه حیات بدین معنی است که یک اتفاق خوب در نهایت رخ خواهد داد. وقتی این ویژگی در یک IBTF مورد استفاده قرار می‌گیرد هر تراکنشی که به شبکه ارسال می‌شود در نهایت به بلاک‌چین همه گره‌های شرکت‌کننده اضافه خواهد شد.

پیاده‌سازی IBFT 1.0 از نظر ایمنی و ادامه حیات دارای نقاط ضعفی بود. از نظر ایمنی، اگر پیشنهاددهنده بیزانس باشد تحت شرایط خاصی می‌تواند از طریق اجماع با مجموعه‌های مختلف، چندین بلوک تأیید شده در

[۱] Safety

[۲] Liveness

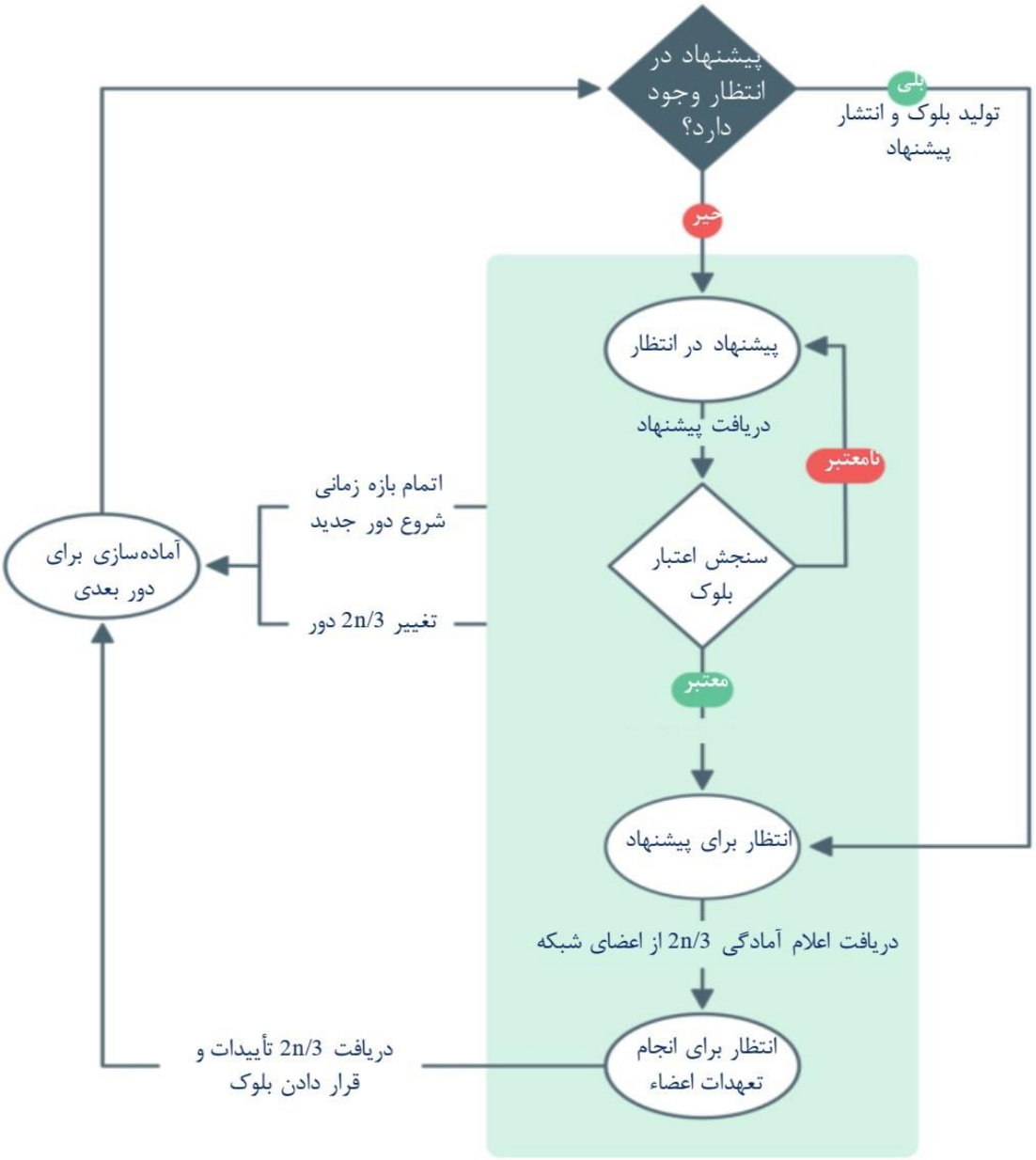
بلاک‌چین یکسان داشته باشد. برای مثال، اگر شبکه پنج اعتبارسنج داشته باشد IBFT 1.0 برای اضافه کردن بلوک به شبکه تنها به توافق سه اعتبارسنج نیاز دارد. همانطور که در شکل زیر نیز نشان داده شده است پیشنهاددهنده بیزانس می‌تواند از طریق اجماع با دو مجموعه مختلف نسبت به تولید دو بلوک متفاوت اقدام کند.



از نظر ویژگی ادامه حیات نیز اگر تنها یک گره بیزانس در شبکه IBFT 1.0 وجود داشته باشد می‌تواند به حالتی برسد که گره‌ها در بلوک‌های متفاوت قفل شوند و دستیابی به توافق در مورد هیچ کدام از بلوک‌ها مقدور نباشد. قفل بلوک‌ها از اضافه شدن بلوک‌های جدید به شبکه جلوگیری می‌کند.

نسخه دوم تحمل خطای بیزانس استانبول (IBFT 2.0)

IBFT 2.0 برای ایجاد نسخه‌های سازمانی پایدار و قابل اعتماد تولید شده است. رویه عملکردی اعتبارسنج‌ها در نسخه دوم تحمل خطای بیزانس استانبول در شکل زیر نشان داده شده است. نیاز به رأی اکثریت، اصلی‌ترین اصلاح ایجاد شده در IBFT 2.0 است که تعداد گره‌های مورد نیاز برای دستیابی به حد نصاب را تغییر می‌دهد. این تغییر، مشکل گره‌های بیزانس در دستیابی به اجماع با دو مجموعه جداگانه از اعتبارسنج‌ها را برطرف کرده است. برای مثال، اگر ۵ اعتبارسنج وجود داشته باشد، IBFT 2.0 با توجه به قاعده رأی اکثریت به جای ۳ اعتبارسنج نسخه قبلی از ۴ اعتبارسنج برای دستیابی به توافق درمورد اضافه کردن بلوک به بلاک‌چین استفاده می‌کند. با این تغییر، یک اعتبارسنج بیزانس نمی‌تواند از دو مجموعه اعتبارسنج درستکار برای دستیابی به توافق درمورد بلاک‌های مختلف استفاده کند.



اصلاح مربوط به تغییر دور[1]، مسئله ادامه حیات در IBFT 1.0 را مرتفع کرده است. در IBFT 1.0 تغییر دور تنها درصورت وجود پیشنهاد بلوک جدید انجام می‌شد. در IBFT 2.0، یک پروتکل تغییر دور پیشرفته تضمین می‌کند که اگر یک اعتبارسنج در یک دور برای تأیید حضور داشته باشد حضور او در هر دور موفق برای آن بلاک ثبت خواهد شد. این مکانیسم که از پروتکل تغییر دیدگاه PBFT الهام گرفته است نیاز به مکانیسم قفل بلوک موجود در نسخه اول IBFT را مرتفع کرده است. مکانیسم قفل بلوک، چالش‌هایی را برای ویژگی ادامه حیات ایجاد می‌کرد.

[1] Round

منابع

[۱] Pegasys, 18 Feb 2019 ”,?Another day, another consensus algorithm. Why IBFT 2.0“ Pegasys. [درون خطی]. Available: https://pegasys.tech/another-day-another-consensus-algorithm-why-ibft-2-0/. [دستیابی در ۸ Aug 2019].

[۲] A. Baliga, P. Kamat و S. Chatterjee ” Performance Evaluation of the Quorum Blockchain Platform,” Persistent Systems Ltd., Pune, India, 2018.

[۳] J. Zhang, “Consensus Algorithms: PoA, IBFT or Raft?,” kaleido, 2018. [درون خطی]. Available: https://kaleido.io/consensus-algorithms-poa-ibft-or-raft/. [دستیابی در ۲۰۱۹].

[۴] Consensys, ”Scaling Consensus for Enterprise: Explaining the IBFT Algorithm“ Consensys, [درون خطی]. Available: https://media.consensys.net/scaling-consensus-for-enterprise-explaining-the-ibft-algorithm-ba86182ea668. [دستیابی در ۲۰۱۹].

[۵] R. Saltini, “Correctness Analysis of IBFT,” PegaSys (ConsenSys), ۲۰۱۹.

کوین ایران

کوین ایران اولین و بزرگ‌ترین پایگاه خبری فارسی زبان در حوزه فناوری بلاک‌چین، رمز ارزها و پلتفرم‌های مرتبط با بلاک‌چین است. این وب سایت در سال ۱۳۹۲ توسط بابک جلیلوند 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 محیط پویای پژوهشی و آموزشی در راستای استفاده صحیح از این فناوری جهت ارائه تسهیلات و رفاه به ایرانیان است.

https://coiniran.com

نویسنده: تورج اکبری

آدرس ایمیل: turaj.akbati68@yahoo.com