

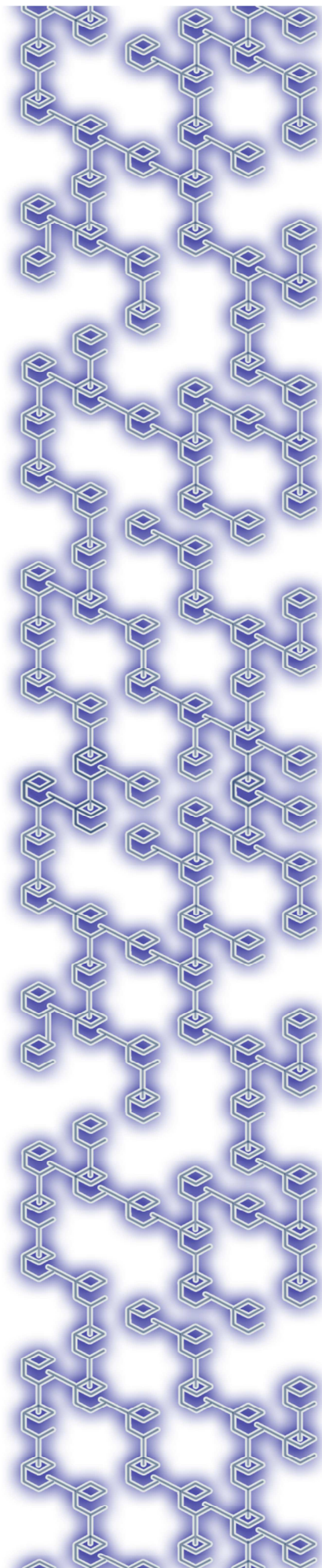
سپیدنامه

شبکه‌ی بلاکچین سور

نسخه ۴

شماره سند: ۹۹۰۱۱۰

تاریخ: ۳۰ شهریور ۱۳۹۹



سپیدنامه بلاکچین سور

«سور» یک پلتفرم قراردادهای هوشمند مبتنی بر ساختار بلاکچین تغییریافته‌ی اتریوم با مقیاس پذیری بالا، زمان بسته شدن بلوک کم، هزینه‌ی تراکنش پایین، دارای خاصیت نهایی سازی فوری^۱ و امکان ثبت تراکنش‌های محرمانه است.

زمان انتشار: ۱۳۹۹/۰۶/۳۰

نگارش: ۴,۳

¹ Immediate Finality

فصل ۱ - مقدمه

با رشد و شکوفایی رمزارزها در سال‌های اخیر، بسیاری این پدیده را تحولی عظیم در دنیای اقتصاد نامیده‌اند و آینده‌ای درخشان برای آن متصور هستند. هرچند، به اعتقاد این افراد رمزارزها هنوز جایگاه واقعی خود در اقتصاد جهانی را پیدا نکرده‌اند، اما این تصور هرگز دور از ذهن نیست.

در کنار استقبال بسیار زیادی که از رمزارزها شده است، عده کثیری از کارشناسان و خبرگان توجه خود را معطوف به فناوری یا در حقیقت تغییر نگرشی که در رمزارزها از آن استفاده شده است، کرده‌اند. این تغییر نگرش به‌طور ویژه حول مفهوم ثبت ایجاد شده است؛ جایی که ثبت رویدادها شامل تراکنش‌ها و غیره به‌صورت غیرمتمرکز و توسط چندین شخص انجام می‌شود. این فناوری که از آن با عنوان بلاکچین یاد می‌شود به‌قدری مورد توجه قرار گرفته است که آن را فناوری تحول‌آفرین چهارم نامیده‌اند.

با داشتن این نگرش به فناوری بلاکچین، اغلب شرکت‌های بزرگ و کوچک از صنایع مختلف در جهت مهار این فناوری گام برداشته‌اند تا بتوانند از مزایای بی‌بدیل آن استفاده کنند؛ اما از آنجا که توسعه‌ی محصولات مبتنی بر بلاکچین از پایه، ساده و ارزان‌قیمت نیست، پرچم‌دار این جنبش جهانی را باید پلتفرم‌های بلاکچینی دانست. در این پلتفرم‌ها که غالباً با هدف گردهمایی علاقه‌مندان و فعالان این فناوری به وجود می‌آیند، خدمات گسترده‌ای شامل کدهای آماده، مشاوره و بستری جامع و کامل برای توسعه‌ی محصولات مبتنی بر بلاکچین در اختیار کاربران قرار می‌گیرد. از مهم‌ترین این پلتفرم‌ها می‌توان اتریوم^۲ و هایپرلجر فابریک^۳ را نام برد که بسیار مورد توجه قرار گرفته‌اند. این پلتفرم‌ها با جذب علاقه‌مندان به فناوری بلاکچین توانسته‌اند اکوسیستمی پویا و کارآمد برای پیشبرد این فناوری به وجود بیاورند.

با وجود تمامی مزایایی که این پلتفرم‌ها از آن برخوردارند، کاربران ایرانی با موانعی جهت استفاده از آن روبه‌رو هستند. برخی از پلتفرم‌ها (اغلب در پلتفرم‌های نیمه‌متمرکز) به دلیل ملاحظات تحریمی از پذیرفتن کاربران ایرانی معذور هستند. حتی در موارد غیرمتمرکزتر مانند پلتفرم اتریوم نیز هزینه‌ی توسعه‌ی یک محصول بر بستر بلاکچین بسیار بالا است (به دلیل تفاوت فاحش ارزش دلار و ریال).

^۲ Ethereum

^۳ Hyperledger Fabric

بنابراین استفاده از این پلتفرم‌ها نیز برای کاربران ایرانی عملاً ناممکن است. وجود معضلات مهمی که ذکر شد و مواردی از این دست، منجر به احساس نیاز به پلتفرم بلاکچینی در داخل کشور به صورت بومی شده است.

با راه‌اندازی پلتفرم بلاکچین سور علاقه‌مندان و فعالان این حوزه می‌توانند بدون دغدغه‌ی مالی و بدون توجه به موانع تحریمی به توسعه‌ی محصول خود بر یک بستر بومی و مبتنی بر نیازهای اقتصادی، اجتماعی و فرهنگی کشور بپردازند. علاوه بر این، پلتفرم سور می‌تواند فعالان مشغول به کار در ارتباط با فناوری بلاکچین از سراسر کشور را که تا امروز به صورت جزیره‌ای عمل کرده‌اند، گرد یک میز بنشاند. به این ترتیب می‌توان انتظار داشت که تعامل نزدیک این اشخاص با یکدیگر قدمی بزرگ در راستای بهره‌مندی کشور از فرصت‌های بی‌نظیر فناوری بلاکچین و در نهایت رشد و شکوفایی اقتصاد ملی باشد.

فصل ۲- تعریف واژگان

● بلاکچین:^۱

«بلاکچین» یا «زنجیره‌ی بلوک» نوعی از ذخیره‌سازی غیر متمرکز داده‌ها است. در یک بلاکچین تراکنش‌های ثبت داده‌ها با امضای دیجیتال افراد صاحب صلاحیت در هر تراکنش، در شبکه جمع آوری می‌شود و در بازه‌های زمانی مشخص، تعدادی از نودها که نقش ثبت تراکنش‌ها را بر عهده دارند، طی یک فرآیند، برای ثبت تعدادی از تراکنش‌ها به توافق می‌رسند و آن تراکنش‌ها را در یک «بلوک» ثبت می‌کنند. عملیات ثبت بلوک از طریق الگوریتم‌های توافق جمعی و مکانیزم «درهم‌کنش» یا هش^۲ انجام می‌شود، تا هر تغییری در یکی از داده‌ها، منجر به تغییر هش کل بلوک گردد. در هر بلوک یک اشاره‌گر هش بلوک قبلی را ذخیره می‌کند و به این ترتیب زنجیره‌ای از بلوک‌ها به وجود می‌آید. پس از ثبت نهایی تراکنش‌ها در بلوک و ثبت شدن تعدادی از بلوک‌ها، احتمال تغییر تراکنش‌ها و محتوای بلوک بسیار کم و در عمل غیر قابل تغییر خواهد بود، زیرا در صورت تغییر یا دستکاری در یک تراکنش لازم است که:

اول: بلوکی که آن تراکنش در آن ثبت شده تغییر کند و بنابراین هش آن بلوک و سپس هش تمام بلوک‌های بعدی به ترتیب تغییر کند.

دوم: برای تأیید این تراکنش نیاز به توافق و تأیید مجدد این بلوک و تمام بلوک‌های بعد از آن توسط نودهای ثبت‌کننده‌ی تراکنش است.

احتمال وقوع این رویداد در یک سیستم غیر متمرکز بسیار بسیار ناچیز خواهد بود.

● قرارداد هوشمند:^۳

اگر در یک بلاکچین این امکان وجود داشته باشد که علاوه بر تراکنش‌های حاوی داده‌ها، برنامه‌های کامپیوتری قابل اجرا نیز در تراکنش‌ها ثبت شوند، قراردادهای هوشمند به وجود می‌آیند. به این ترتیب نودهای ثبت تراکنش‌ها، می‌توانند توابع این قراردادهای هوشمند را اجرا کنند و نتایج را در بلاکچین ثبت کنند یا آن را در اختیار متقاضیان قرار دهند. در این

^۱ Blockchain

^۲ Hash

^۳ Smart Contract

صورت تمام خواص مطلوب در بلاکچین از قبیل شفافیت، قابلیت اثبات، حفظ تاریخچه، عدم امکان تغییر در تراکنش‌های ثبت شده، غیر قابل جعل بودن و ... به برنامه‌های کامپیوتری مورد نظر و اجرای آنها نیز منتقل می‌شود.

به این ترتیب قرارداد هوشمند افق جدیدی را پیش روی سازمان‌ها و کسب‌وکارها قرار می‌دهد تا از امکانات آن استفاده نمایند.

به عنوان مثال می‌توان از قراردادهای هوشمند برای ثبت گواهی‌های تحصیلی، اداری و حرفه‌ای، ثبت اسناد مالکیت، ثبت موالید، مدیریت زنجیره‌ی تأمین، بیمه و طیف وسیعی از انواع کسب‌وکارها و خدمات استفاده کرد.

● **توابع قراردادهای هوشمند:**

یک قرارداد هوشمند به طور معمول علاوه بر داده‌ها از تعدادی تابع که حاوی برنامه‌های رایانه‌ای به زبان‌های خاص است، تشکیل شده است. این تابع‌ها وظایف آن قرارداد هوشمند را انجام می‌دهند. هر فرد مجاز که در قرارداد هوشمند به وی اجازه داده شده باشد، می‌تواند تابع مورد نظر را اجرا کند.

● **ثبت بلوک:**

هنگامی که نودهای ثبت‌کننده‌ی تراکنش‌ها در بلاکچین، طبق الگوریتم مشخص شده در نهایت برای ثبت تعدادی تراکنش به توافق می‌رسند، یک بلوک از تراکنش‌ها تشکیل می‌شود و بلوک به ثبت می‌رسد و همه‌ی نودهای شبکه، بلوک ثبت‌شده را به عنوان آخرین بلوک بلاکچین می‌پذیرند و آن را ذخیره می‌کنند.

● **پاداش ثبت بلوک:**^۱

وقتی که نودهای ثبت‌کننده‌ی تراکنش‌ها در بلاکچین، برای ثبت تعدادی تراکنش در یک بلوک به توافق می‌رسند، به طور معمول به نود پیشنهاد دهنده‌ی آن بلوک مقداری توکن شبکه به عنوان پاداش داده می‌شود. این توکن‌ها اغلب در طی همان روند به وجود می‌آیند.

● **اجماع:**^۲

^۱ Block Reward

^۲ Consensus

الگوریتمی که نودهای ثبت‌کننده‌ی تراکنش‌ها در یک بلاکچین برای به توافق رسیدن به کار می‌برند، الگوریتم اجماع نامیده می‌شود. برای اشاره به بعضی از الگوریتم‌های رایج برای اجماع، می‌توان الگوریتم اثبات کار^۱، الگوریتم اثبات سهام^۲ و الگوریتم اثبات اقتدار^۳ را برشمرد.

● توکن^۴:

توکن‌ها اغلب به عنوان نماینده‌ی یک دارایی در بلاکچین مورد استفاده قرار می‌گیرند. به عنوان نمونه یک توکن می‌تواند نماینده‌ی مقدار مشخصی از کالای خاص باشد، یا فقط به عنوان یک دارایی برای دریافت خدمات مشخص به کار رود. مثالی از یک توکن در دنیای خارج از بلاکچین بلیط اتوبوس یا سینما یا ژتون یک رستوران باشد.

● توکن پایه‌ی شبکه^۵:

در یک شبکه‌ی بلاکچین که قابلیت پیاده‌سازی قراردادهای هوشمند را دارا است، می‌توان با استفاده از قراردادهای هوشمند توکن‌هایی را در شبکه به وجود آورد. اما «توکن پایه‌ی شبکه» توکنی است که با استفاده از آن می‌توان قراردادهای هوشمند را به وجود آورد یا توابع آن را اجرا کرد. به عنوان نمونه در شبکه‌ی بلاکچین اتریوم، توکن پایه‌ی شبکه اتر نامیده می‌شود. اما در همین شبکه توکن‌های دیگری نیز وجود دارند که با استفاده از قراردادهای هوشمند به وجود آمده‌اند. به عنوان مثالی از توکن‌های دیگر شبکه می‌توان به توکن تتر^۶ اشاره کرد.

● دپ^۷:

دپ یا «برنامه‌ی کاربردی غیرمتمرکز» عبارت است از یک برنامه‌ی کاربردی که در یک بستر ارتباطی غیرمتمرکز اجرا می‌شود. امروزه بیشتر دپ‌ها از بلاکچین و قراردادهای هوشمند برای ذخیره‌سازی، خواندن و مدیریت دسترسی داده‌های خود استفاده می‌کنند.

● پلتفرم^۸:

یک پلتفرم، مجموعه‌ای از سخت‌افزار، نرم‌افزار و ارتباطات شبکه‌ای است که از طریق ایجاد تعامل بین تولیدکنندگان محصولات یا خدمات یا محتوا با مصرف‌کنندگان، ارزش‌آفرینی می‌کند.

^۱ POW: Proof Of Work

^۲ POS: Proof Of Stake

^۳ POA: Proof Of Authority

^۴ Token

^۵ Native Token

^۶ Tether

^۷ DApp: Decentralized Application

^۸ Platform

فصل ۳- زیرساخت‌های مشابه

برای پیاده‌سازی قراردادهای هوشمند روی یک بلاکچین عمومی، در حال حاضر زیرساخت‌های مختلفی در دسترس کاربران قرار دارد. بعضی از این زیرساخت‌ها در این فصل معرفی شده‌اند.

۳-۱- اتریوم^۱

در سال ۲۰۱۳ یک برنامه‌نویس جوان روسی کانادایی به نام ویتالیک بوتیرین^۲ سپیدنامه‌ی اتریوم را منتشر کرد و پلتفرم قرارداد هوشمند را به جهان معرفی کرد. ایده‌ی اصلی این پلتفرم ساخت یک ابررایانه‌ی جهانی برای اجرای قراردادهای هوشمند است. راه‌اندازی این شبکه در سال ۲۰۱۵ انجام شد. بر مبنای این طرح، بلاکچین از نظر فناوری یک گام به پیش نهاد و علاوه بر ثبت تراکنش‌ها و داده‌ها ثبت و اجرای برنامه‌های کامپیوتری را نیز عهده‌دار شد و به این ترتیب هسته‌ی اولیه‌ی اپلیکیشن‌های غیرمتمرکز^۳ متولد شد.

در شبکه‌ی اتریوم توکن پایه‌ی شبکه به نام اتر برای پرداخت کارمزد تراکنش‌ها به کار می‌رود. جدول ۱ اطلاعات کلی در مورد توکن اتر و شبکه‌ی اتریوم ارائه می‌دهد.

جدول ۱- مشخصات بلاکچین اتریوم و توکن آن

نام توکن اصلی شبکه	اتر (Ether)
نام اختصاری توکن اصلی شبکه	ETH
تعداد توکن تولیدشده‌ی اولیه	۷۲ میلیون اتر
زمان تشکیل هر بلوک	۱۵ ثانیه
پاداش ثبت بلوک	۲ اتر

^۱ Ethereum

^۲ Vitalik Buterin

^۳ DAPP: Decentralized Application

تعداد توکن موجود تاکنون	۱۱۱ میلیون اتر
ظرفیت تراکنش موجود	۲۵ تراکنش در ثانیه
الگوریتم اجماع	اثبات کار (POW)

سپیدنامه‌ی اتریوم^۱ و سایت رسمی اتریوم^۲ اطلاعات بیشتری در اختیار خواننده قرار می‌دهند.

۳-۲-۳ ترون

طرح اصلی ترون در سال ۲۰۱۷ توسط جاستین سان^۴، کارآفرین چینی بنیانگذاری شد و در سال ۲۰۱۸ شبکه‌ی بلاکچین مستقل خود را راه‌اندازی کرد.

ایده‌ی پروژه‌ی ترون راه‌اندازی یک بلاکچین با امکان اجرای قرارداد هوشمند با مقیاس‌پذیری بالا و کارمزد کم است. در حال حاضر شبکه‌ی بلاکچین ترون مانند اتریوم از زبان سالیدیتی برای پیاده‌سازی قراردادهای هوشمند استفاده می‌کند. اطلاعات بیشتر در این مورد در جدول ۲ آمده است.

جدول ۲- مشخصات بلاکچین ترون و توکن آن

نام توکن اصلی شبکه	ترون
نام اختصاری توکن اصلی شبکه	TRX
تعداد توکن تولیدشده‌ی اولیه	۱۰۰ میلیون
زمان تشکیل هر بلوک	۱۵ ثانیه
پاداش ثبت بلوک	۱۶ ترون
تعداد توکن موجود تاکنون	۶۶ میلیارد
ظرفیت تراکنش موجود	۲۰۰۰ تراکنش در ثانیه

^۱ <https://ethereum.org/whitepaper>

^۲ <https://ethereum.org>

^۳ Tron

^۴ Justin Sun

اثبات سهام وکالتی (DPOS)	الگوریتم اجماع
--------------------------	----------------

۳-۳-۱- ای‌اواس^۱

ای‌اواس بر پایه‌ی نرم‌افزار ای‌اواس‌آی‌او^۲ توسط شرکت «بلاک وان» ساخته شده‌است. بلاک وان توسط «برندان بلومر»^۳ و «دنیل لاریمر»^۴ رهبری می‌شود. او مبدع روش اجماع اثبات سهام وکالتی^۵ و سازمان خودمختار غیرمتمرکز، معروف به دائو^۶ است. او کسی است که پشت «بیت شیرز»^۷ و «استیم»^۸ قرار دارد. شبکه‌ی اصلی ای‌اواس در سال ۲۰۱۸ راه اندازی شد.

ای‌اواس حمایت از برنامه‌های غیرمتمرکز را در مقیاس صنعتی هدف قرار داده‌است. روشی که آنها قصد انجام آن را دارند، نزدیک شدن به قراردادهای هوشمند از یک زاویه‌ی متفاوت نسبت به اتریوم است. ای‌اواس به جای یک ابررایانه‌ی غیر متمرکز، قصد دارد یک سیستم‌عامل غیر متمرکز باشد. کاربران در ای‌اواس در ازای سهم خود از ای‌اواس منابع سیستم را به دست خواهند آورد. بنابراین، اگر یک‌هزارم از سهام ای‌اواس را در اختیار داشته باشید، مالکیت یک هزارم از کل توان محاسباتی و منابع موجود در ای‌اواس را خواهید داشت. اطلاعات بیشتر در این زمینه جدول ۳ آمده است.

جدول ۳- مشخصات بلاکچین ای‌اواس و توکن آن

ای‌اواس	نام توکن اصلی شبکه
EOS	نام اختصاری توکن اصلی شبکه
۱۰۰ میلیون	تعداد توکن تولیدشده‌ی اولیه
۰,۵ ثانیه	زمان تشکیل هر بلوک
هر سازنده‌ی بلاک ۱۰۰ توکن در	پاداش ثبت بلوک

^۱ EOS

^۲ EOSIO

^۳ Brendan Blumer

^۴ Daniel Larimer

^۵ DPOS: Delegated Proof Of Stake

^۶ DAO: Decentralized Autonomous Organization

^۷ BitShares

^۸ Steem

روز	
تعداد توکن موجود تاکنون	۹۳۲ میلیون
ظرفیت تراکنش موجود	۴۰۰۰ تراکنش در ثانیه
الگوریتم اجماع	اثبات سهام وکالتی (DPOS)

۳-۴- کاردانو^۱

کاردانو یکی از پروژه‌های فضای رمزارزها است که زیاد در مورد آن سخن گفته می‌شود و مقیاس‌پذیری و امنیت را از طریق معماری لایه‌ای ارائه می‌دهد. ایده‌ی اصلی این پروژه توسط یکی از بنیان‌گذاران پروژه‌ی اتریوم به نام چارلز هاسکینسون^۲ پیشنهاد شد و در سال ۲۰۱۷ شبکه‌ی اصلی آن راه‌اندازی گردید.

رویکرد کاردانو در فضای رمزارزها نیز منحصر به فرد است، زیرا بر روی فلسفه‌ی علمی و تحقیقات دانشگاهی ساخته شده‌است. هدف نهایی این پروژه پیدا کردن تعادل عالی بین ارائه‌ی خدمات به کاربران و همچنین قانونگذاران می‌باشد. تیم کاردانو احساس می‌کند که این موضوع به آن خاطر مهم است که نهایتاً، ارز رمزنگاری شده به نحوی وارد صنعت مالی خدمات خواهد شد. اطلاعات بیشتر در مورد این بلاکچین در جدول ۴ آمده است.

جدول ۴- مشخصات بلاکچین کاردانو و توکن آن

نام توکن اصلی شبکه	کاردانو
نام اختصاری توکن اصلی شبکه	ADA
تعداد توکن تولیدشده‌ی اولیه	۵ میلیارد
زمان تشکیل هر بلوک	۲۰ ثانیه
پاداش ثبت بلوک	۷۹۸ توکن

^۱ Cardano

^۲ Charles Hoskinson

تعداد توکن موجود تاکنون	۹۳۲ میلیون
ظرفیت تراکنش موجود	۲۵۷ تراکنش در ثانیه
الگوریتم اجماع	نوعی از اثبات سهام وکالتی به نام اوروبوروس (Ouroboros)

۳-۵-آلاستریا^۱

از شبکه‌ی آلاستریا در ماه می سال ۲۰۱۷ رونمایی شد. این اکوسیستم غیرانتفاعی متشکل از بیش از ۷۰ شرکت اسپانیایی می‌باشد. آلاستریا یک زیرساخت بلاکچینی و دارای عملکرد قراردادهای هوشمند، هویت دیجیتال و امنیت داده‌ها مطابق با مقررات اروپا است، اما مهم‌تر از همه یک روش استاندارد برای جریان اطلاعات بین اعضای این کنسرسیوم است.

از آنجا که کنسرسیوم شامل مؤسساتی از قبیل بانک‌ها، دانشگاه‌ها، قانون‌گذاران، شرکت‌های فن‌آوری و غیره است، یک شبکه‌ی استاندارد مبتنی بر بلاکچین به توسعه‌دهندگان کمک خواهد کرد تا برنامه‌هایی بسازند که سازگار و عملیاتی در میان این مؤسسات باشد.

ویژگی مهم دیگر این کنسرسیوم این است که جدای از همکاری بخش خصوصی - خصوصی (مانند دبی) امکان مشارکت دانشگاه‌ها و مهم‌تر از قانون‌گذاران وجود دارد. گاهی اوقات، داشتن تعداد زیادی بازیکن می‌تواند منجر به کند شدن روند پیشرفت شود، اما وجود اعضای آکادمیک و افراد حرفه‌ای همراه با اعضای نوآور و قانونگذاران، سبب حرکت شتابان به سمت پیشرفت می‌شود.

بلاکچین آلاستریا یک بلاکچین عمومی^۲ و نیازمند مجوز^۳ است و براساس یک توسعه از اتریوم به نام کوروم^۴ استقرار یافته است.

۳-۶-مقایسه‌ی زیرساخت‌های معرفی شده

در جدول ۵ اطلاعات مقایسه‌ای زیرساخت‌هایی که در این فصل معرفی شدند، آمده است:

^۱ Alastria

^۲ Public Blockchain

^۳ Permissioned Blockchain

^۴ Quorum

جدول ۵- مقایسه‌ی مشخصات بلاکچین‌های ذکرشده

عامل مقایسه	اتریوم	ترون	ای‌اواس	کاردانو	آلستریا
استفاده از شبکه	عمومی	عمومی	عمومی	عمومی	عمومی
ثبت نهایی	بدون نیاز به مجوز	نیاز به مجوز	نیاز به مجوز	نیاز به مجوز	نیاز به مجوز
نام توکن اصلی شبکه	اتر	ترون	ای‌اواس	کاردانو	بدون توکن
نام مخفف توکن اصلی شبکه	ETH	TRX	EOS	ADA	بدون توکن
روش اجماع در حال حاضر	POW	DPOS	DPOS	Ouroboros	RAFT
زبان برنامه‌نویسی منبع	Go	Java	C++	Haskell	Go
زبان برنامه‌نویسی قرارداد هوشمند	Solidity	Solidity	WASM	Plutus	Solidity
حداکثر تعداد تراکنش در ثانیه	15-25	2000	4000	50-250	1500
زمان متوسط بلاک (ثانیه)	15	3	0.5	<20	1
متوسط هزینه‌ی هر تراکنش ساده (دلار)	0.28	0.0005	0.05	0.05	رایگان
توانایی ارائه‌ی تراکنش‌های محرمانه	خیر	خیر	خیر	خیر	بلی

فصل ۴ – معرفی پلتفرم سور

۴-۱ – معماری پلتفرم سور

پلتفرم سور بر اساس معماری «هایپرلجربسو»^۱ با تغییراتی در متن برنامه‌ی آن بنا شده است.^۲ برای آشنایی بیشتر با هایپرلجربسو به ضمیمه‌ی ۱ مراجعه کنید.

۴-۱-۱ – مشخصات پلتفرم سور

در این پلتفرم، مانند هایپرلجربسو با استفاده از زبان سالیدیتی می‌توان قراردادهای هوشمند را بر روی بلاکچین پیاده‌سازی کرد و با استفاده از آن اپلیکشن‌های غیرمتمرکز را در حوزه‌های مختلف راه‌اندازی کرد.

در پلتفرم بلاکچین سور در هر ۲ ثانیه یک بلوک جدید بسته می‌شود. سائز بلوک‌ها از نظر حجمی محدودیت خاصی ندارد، اما مقدار گس مصرفی در هر بلوک حداکثر می‌تواند ۱۰ میلیون واحد گس باشد. کارمزد تراکنش‌ها دقیقاً مانند شبکه‌ی بلاکچین اتریوم است.

برخی مشخصات بنیادین پلتفرم سور در جدول ۶ آمده است:

جدول ۶- مشخصات اساسی پلتفرم بلاکچین سور

مشخصه	مقدار	توضیح
بیشینه‌ی اندازه‌ی بلوک	نامحدود	اندازه‌ی هر بلوک به جای حجم با سوخت مصرفی محدود می‌شود

^۱ Hyperledger BESU

^۲ به عنوان مرجع معتبر در مورد هایپرلجربسو به این لینک مراجعه کنید: <https://besu.hyperledger.org/en/latest/>

مشخصه	مقدار	توضیح
زمان تشکیل هر بلوک	۲ ثانیه	
بیشینه‌ی سوخت مصرفی هر بلوک	۱۰ میلیون گس	
پاداش ثبت هر بلوک	متغیر	در ابتدا ۱,۲۷ توکن است و طی یک روند ۲۰ ساله به صفر می‌رسد.
الگوریتم اجماع	IBFT-2	
تعداد تأییدکننده‌های اولیه	۱۳	

۴-۱-۲- اجماع در پلتفرم سور

در پلتفرم سور از الگوریتم اجماع IBFT 2.0 استفاده می‌شود که در آن تصمیم‌گیری با تعداد دقیق

حداقل $a = \left\lceil \frac{2n+2}{3} \right\rceil$ رأی از کل آرا (n) صورت می‌پذیرد.

در این پلتفرم تعدادی نود به عنوان تأییدکننده^۱ تراکنش‌های ثبت قرارداد هوشمند، اجرای توابع قرارداد هوشمند و نیز انتقال توکن را در شبکه تأیید می‌کنند. به این ترتیب که تأیید تراکنش به صورت چرخشی بین نودهای شبکه تقسیم می‌شود و در صورت عدم آمادگی آن نود، نوبت به نود بعدی در حلقه می‌رسد. سایر نودهای شبکه (که در یک بلوک نوبتشان نرسیده است) نیز تراکنش‌های ثبت شده را بررسی و در سیستم خود ثبت می‌کنند.

۴-۱-۳- جذب یا اخراج تأییدکنندگان

پلتفرم بلاکچین سور توسط بنیادی به نام بنیاد بلاکچین سور راه‌اندازی می‌شود و بنیاد بر حسن کارکرد بلاکچین و اجرای قواعد مصوب نظارت خواهد نمود. این بنیاد در فصل ۵ معرفی خواهد شد.

¹ Validator

در ابتدای کار پلتفرم تعدادی از فعالان بازار بلاکچین ایران که از اعضای بنیاد سور نیز هستند به‌عنوان تأییدکنندگان شبکه این کار را آغاز خواهند کرد. اما بنیاد تلاش خواهد کرد تا بیش از نیمی از تعداد تأییدکنندگان عضو بنیاد، افراد حقیقی و حقوقی با بیشترین تضاد منافع از خارج بنیاد به‌عنوان تأییدکننده جذب کند. به این ترتیب، سهم تأییدکنندگان عضو بنیاد کمتر از دوسوم کل تأییدکنندگان خواهد شد و بنیاد نقش بدون منازع در افزودن یا خارج کردن تأییدکنندگان دیگر نخواهد داشت.

بنیاد همچنین آیین‌نامه‌ی شرایط پذیرش تأییدکنندگان جدید را تصویب و ابلاغ خواهد نمود. برای افزودن تأییدکننده‌ی جدید نیز بین نودهای فعلی رأی‌گیری می‌شود و در صورت تأیید حدود ۶۷٪ تأییدکننده‌ها (طبق اجماع IBFT-2) نود جدید به‌عنوان تأییدکننده در سیستم پذیرفته می‌شود. به همین ترتیب با اجماع تأییدکننده‌های موجود، می‌توان یک تأییدکننده را از بلاکچین خارج کرد.

۴-۱-۴- توکن پایه‌ی شبکه

پرداخت کارمزد تراکنش‌ها در شبکه‌ی بلاکچین سور با استفاده از توکن پایه‌ی شبکه به نام «سورن» انجام می‌شود. در قسمت‌های بعد در مورد این توکن توضیح بیشتر ارائه خواهد شد.

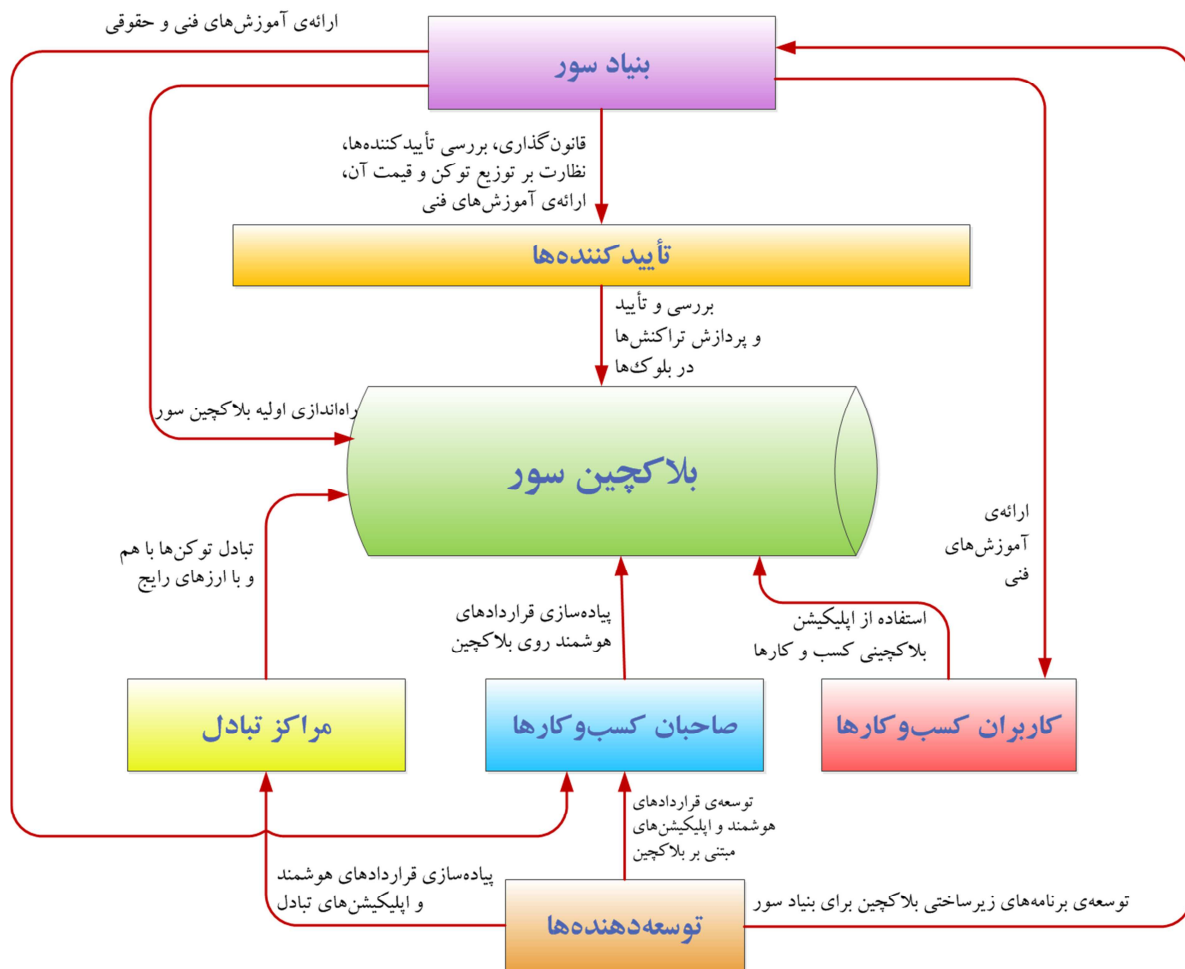
۴-۱-۵- مدل مفهومی پلتفرم سور

اگر بخواهیم تعامل دست اندرکاران مختلف در پلتفرم سور را با یکدیگر بررسی کنیم، می‌توانیم از نمودار شکل ۱ کمک بگیریم.

تعریف و وظایف هریک از طرف‌ها در نمودار شکل ۱ در بخش ۴-۱-۶ تشریح شده است.

۴-۱-۶- ذینفعان پلتفرم سور

طرف‌های درگیر در پلتفرم سور و وظایف و اختیارات آنها را می‌توان به این ترتیب بررسی کرد:



شکل ۱- مدل مفهومی دست اندرکاران بلاکچین سور

۴-۱-۶-۱- بنیاد سور

بنیاد سور مؤسسه‌ی ثبت‌شده‌ای است که متشکل از افراد حقیقی و حقوقی مؤسس شبکه‌ی بلاکچین سور است. بنیاد سور در فصل ۵ معرفی خواهد گردید. وظایف بنیاد سور به طور مشروح در فصل ۵ آمده است.

۴-۱-۶-۲- تأییدکننده‌ها^۱

تأییدکننده همان طور که گفته شد به نودهایی گفته می‌شود که صحت تراکنش‌های شبکه را بررسی می‌کنند و تراکنش‌ها را در بلوک ثبت می‌نمایند.

وظایف هر تأییدکننده را می‌توان به ترتیب زیر فهرست نمود:

- بررسی صحت تراکنش‌های ارسال شده به شبکه
- ثبت تراکنش‌های صحیح ارسال شده در بلوک
- ثبت و نهایی‌سازی بلوک تشکیل‌شده

۴-۱-۶-۳- صاحبان کسب‌وکارها

صاحبان کسب‌وکارها شامل طیف وسیعی از شرکت‌ها و بنگاه‌های اقتصادی و غیر اقتصادی بزرگ و کوچک و استارت‌آپ‌ها و شرکت‌های دانش‌بنیان و نیز کارآفرینان فردی هستند که برای ارائه‌ی خدمات خود به استفاده از بلاکچین نیاز دارند. آنان می‌توانند طرح استفاده از بلاکچین خود را برای دریافت مشاوره‌های حقوقی و فنی با بنیاد سور مطرح کنند و یا خود به طور مستقیم طرح خود را روی شبکه‌ی سور اجرا کنند. بدیهی است در صورت پیاده‌سازی قراردادهای هوشمندی که استفاده از آنها با قوانین مغایرت داشته باشد، بنیاد سور طبق تعریف این حق را دارد که قرارداد هوشمند مزبور را در صورت وجود حکم قضایی روی بلاکچین مسدود نماید.

بنا بر موارد فوق حتی کاربران شخصی نیز می‌توانند نیازهای خود را در صورت لزوم با استفاده از قراردادهای هوشمند بر روی بلاکچین سور ایجاد کنند.

صاحبان کسب‌وکارهای بلاکچینی، وظایف زیر را در این شبکه بر عهده دارند:

- انطباق دادن کسب‌وکار خود با قوانین و مقررات
- تهیه و پیاده‌سازی قراردادهای هوشمند بر مبنای طرح کسب‌وکار با همکاری توسعه‌دهندگان
- تبلیغ و بازاریابی کسب‌وکار برای جذب کاربران بیشتر طبق طرح بازاریابی خود

¹ Validator

۴-۱-۶-۴- کاربران کسب‌وکارها

کاربران کسب‌وکارها یکی از ارکان مهم شبکه هستند. آنان از کاربردهایی که کسب‌وکارهای مختلف روی شبکه ایجاد می‌کنند، استفاده می‌کنند.

کاربران به کسب‌وکارهای مورد علاقه‌ی خود می‌پیوندند و نیازهای روزمره‌ی خود را با استفاده از آن برآورده می‌سازند.

کاربران کسب‌وکارها وظایف زیر را انجام می‌دهند:

- عضویت در اپلیکیشن‌های کسب‌وکار مورد نظر خود و در صورت لزوم احراز هویت
- برآوردن نیازهای روزمره با استفاده از اپلیکیشن‌های مورد نظر

۴-۱-۶-۵- مراکز تبادل^۱

مراکز تبادل سایت‌هایی هستند که کار آنها تبادل توکن پایه‌ی شبکه‌ی سور، به نام سورن، با پول‌های رایج نظیر ریال است. مراکز تبادل همچنین می‌توانند توکن‌های خدماتی خاص را که کسب‌وکارهای شبکه برای نیازهای خود تعریف کرده‌اند، با پول‌های رایج و نیز با خود سورن، مبادله کنند.

وظایف سایت‌های مرکز تبادل را می‌توان از قرار زیر برشمرد:

- احراز هویت کاربران سایت
- ثبت سفارش‌های خرید مربوط به هر جفت‌ارز
- ثبت سفارش‌های فروش مربوط به هر جفت‌ارز
- انطباق سفارش‌های خرید با فروش طبق قواعد تعیین شده
- بازگرداندن توکن‌ها و پول‌های مبادله به کاربران پس از کسر کارمزد مبادلات

کاربران مراکز تبادل می‌توانند هر یک از طرف‌هایی باشند که نیاز به مبادله‌ی توکن با پول یا توکن با توکن دارند. به عنوان مثال، کاربران کسب‌وکارها کسانی هستند که معمولاً نیاز به خرج کردن توکن در اپلیکیشن‌های کسب‌وکارها دارند و به همین دلیل مایلند که ریال را به توکن مربوطه تبدیل نمایند. در

¹ Exchange

مقابل توکن‌های خرج‌شده در شبکه به کاربران دیگر یا صاحبان کسب‌وکارها می‌رسد و آنان تمایل دارند که توکن‌های به دست آمده را به ریال تبدیل نمایند.

۴-۱-۶- توسعه‌دهنده‌ها

توسعه‌دهنده‌ها برنامه‌های زیرساختی و کاربردی شبکه نظیر کاوشگر^۱، کیف توکن^۲، نودهای شبکه^۳، قراردادهای هوشمند و اپلیکیشن‌های لازم برای کسب‌وکارها، سازمان‌های دولتی و بنیاد سور را تولید می‌کنند و در ازای آن توکن سورن یا ریال دریافت می‌کنند.

وظایف توسعه‌دهنده‌ها در شبکه از قرار زیر است:

- توسعه‌ی برنامه‌های لازم طبق سفارش و بر مبنای توافق قیمت با کارفرما

۴-۱-۷- ارتباط داده‌ای بین ذینفعان

تبادل داده‌ها و اطلاعات بین طرف‌های دخیل در پلتفرم سور در قالب‌های خاصی صورت می‌پذیرد. خلاصه‌ای از روندهای تبادل داده‌ی مستقیم و غیرمستقیم با بلاکچین سور در نمودار شکل ۲ آمده است. مشروح ارتباط داده بین ذینفعان بلاکچین سور از قرار زیر است:

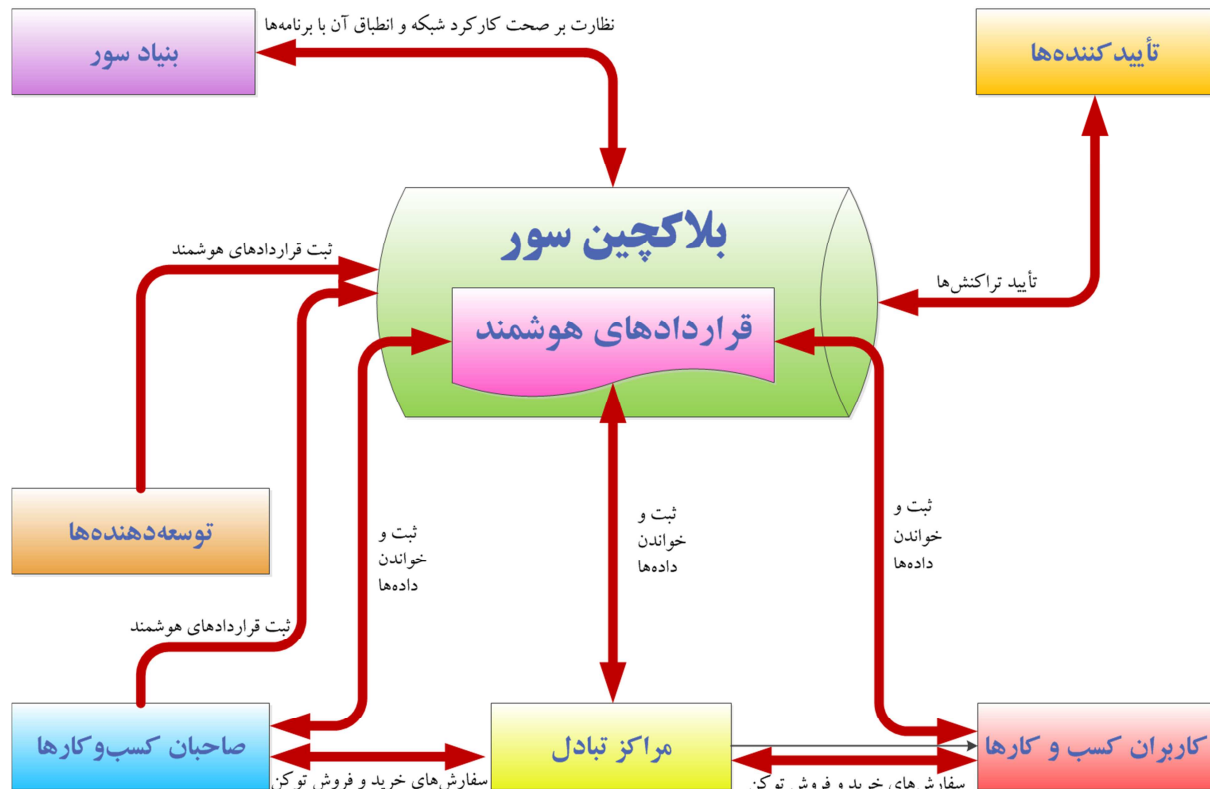
- تأییدکننده‌ها^۴ طبق تعریف وظایف اولیه، اطلاعات مربوط به تراکنش‌های ارسال شده به شبکه را دریافت می‌کنند و در صورت صحت تراکنش‌ها طبق قواعد شبکه، آنها را در بلوک بعدی بلاکچین ثبت نهایی می‌کنند.
- صاحبان کسب‌وکارها نیز قراردادهای هوشمند مربوط به کسب‌وکار خود را در شبکه ثبت می‌کنند، اطلاعات ثبت شده در قرارداد هوشمند مربوط به کسب‌وکار خود را به‌روز می‌کنند و تراکنش‌های لازم برای کسب‌وکار خود را ثبت می‌کنند.

^۱ Explorer

^۲ Wallet

^۳ Blockchain Nodes

^۴ Validator



شکل ۲- ارتباط داده‌ای بین ذینفعان شبکه‌ی بلاکچین سور

- کاربران کسب و کارها نیز طبق تعریف قواعد هر کسب و کار تراکنش‌های مربوط به آن را در شبکه ثبت می‌کنند و داده‌های مربوط به آن را از شبکه دریافت می‌کنند.
- سایت‌های مرکز تبادل نیز تبادل نهایی توکن‌ها را در قراردادهای هوشمند مربوط به هر توکن در شبکه ثبت می‌کنند.
- توسعه دهنده‌ها نیز قراردادهای هوشمند مربوط به سفارش‌های دریافتی خود را روی بلاکچین ثبت می‌نمایند.

۴-۲- اقتصاد بلاکچین سور

پلتفرم سور مانند پلی میان توسعه دهنده‌ها، کاربران و ایده پردازان عمل خواهد کرد. ایده پردازان می‌توانند ایده‌های کسب و کار مبتنی بر بلاکچین خود را از طریق توسعه دهنده‌ها و بر بستر بلاکچین سور در اختیار کاربران قرار دهند.

مشروح ارتباط مالی بین طرف‌های مختلف در این پروژه در قسمت ۴-۲-۳ آمده است.

۴-۲-۱- توکن پایه‌ی شبکه

شبکه‌ی بلاکچین سور دارای یک توکن پایه‌ی شبکه به نام سورن^۱ است. این توکن برای پرداخت هزینه‌ی ثبت تراکنش‌ها از سوی ثبت‌کننده‌ی تراکنش پرداخت می‌شود و در نهایت توسط تأییدکننده‌ای که این تراکنش توسط وی ثبت می‌شود، دریافت می‌شود. به این ترتیب چرخه‌ی گردش توکن شبکه تعریف می‌شود.

۴-۲-۲- توکن‌های قابل تعریف برای کسب‌وکارهای مختلف روی شبکه

هر کسب‌وکار روی شبکه‌ی بلاکچین سور می‌تواند برای راه‌اندازی اقتصاد خود یک توکن همسان و قابل مبادله تعریف کند. شیوه‌ی ارزش‌گذاری این توکن‌ها توسط صاحبان کسب‌وکارها تعیین می‌شود.

توکن‌های همسان^۲ و قابل مبادله که ارزش آنها در بازار عرضه و تقاضا تعیین می‌شود، می‌توانند در سایت‌های مرکز تبادل نیز با توکن‌های دیگر و نیز با پول ریال مبادله شوند.

توکن‌های قابل مبادله می‌توانند با استاندارد ERC-20^۳ یا هر یک از توسعه‌های آن در شبکه‌ی بلاکچین سور ساخته و توزیع شوند.

علاوه بر آن هر کسب‌وکار می‌تواند برای منظوره‌ای خاص خود از توکن‌های ناهمسان^۴ نیز استفاده کند. مثال‌هایی از توکن‌های ناهمسان امتیازهایی که به کسی داده می‌شود یا گواهی‌نامه‌های تحصیلی یا مهارتی که از سوی مؤسسات ارائه می‌شود. توکن‌های ناهمسان می‌توانند قابل مبادله یا غیر قابل مبادله باشند که حتی در صورت قابل مبادله بودن، مبادله‌ی آن در مراکز تبادل معمول قابل انجام نیست. استاندارد ERC-721^۵ یا معادل‌های آن در مورد توکن‌های ناهمسان است.

^۱ سورن (SUREN) یا سورنا یکی از سرداران بزرگ و نامدار تاریخ در زمان اشکانیان است که سپاه ایران را در نخستین جنگ با رومیان فرماندهی کرد و رومی‌ها را که تا آن زمان در همه جا پیروز بودند، برای اولین بار با شکستی سخت و تاریخی روبرو ساخت.

^۲ Fungible Tokens

^۳ جهت آشنایی بیشتر با استاندارد ERC-20 به این منبع مراجعه کنید: <https://eips.ethereum.org/EIPS/eip-20>

^۴ Nonfungible Tokens

^۵ جهت آشنایی بیشتر با استاندارد ERC-721 به این منبع مراجعه کنید: <https://eips.ethereum.org/EIPS/eip-721>

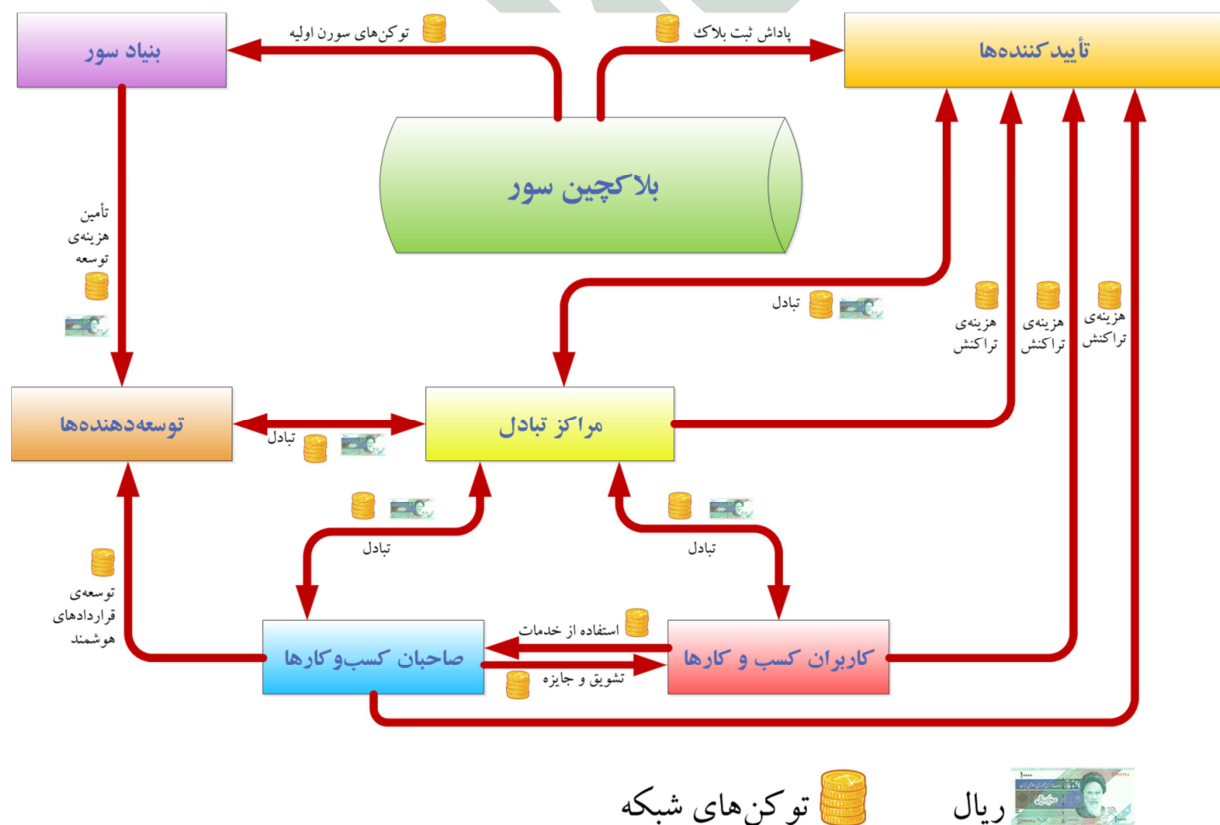
۴-۲-۳- ارتباط مالی طرف‌های مختلف شبکه با یکدیگر

طرف‌های مختلف در شبکه‌ی بلاکچین سور، به اقتضای نقش خود در شبکه با دیگر طرف‌های شبکه مبادلاتی دارند. خلاصه‌ای از این مبادلات در نمودار شکل ۳ دیده می‌شود.

۴-۲-۳-۱- روابط مالی بنیاد سور

بنیاد سور در هنگام نصب اولیه‌ی شبکه‌ی بلاکچین سور، تعدادی توکن اولیه‌ی سورن تعریف کرده است. این توکن‌ها برای مقاصد زیر استفاده می‌شوند:

- تأمین هزینه‌های لازم برای توسعه و به‌روزرسانی شبکه
- تأمین هزینه‌های جاری بنیاد
- تأمین هزینه‌های ترویج و آموزش شبکه



شکل ۳- ارتباط مالی ذینفعان شبکه‌ی بلاکچین سور با یکدیگر

۴-۲-۳-۲- روابط مالی تأییدکننده‌ها^۱

تأییدکننده‌ها در بلاکچین سور نقش پایدارسازی شبکه و ثبت و نگهداری تراکنش‌ها در بلوک‌های شبکه را بر عهده دارند. هزینه‌های تأییدکننده‌ها از دو محل تأمین می‌شود:

- پاداش ثبت بلوک: هر تأییدکننده بابت ثبت هر بلوک در زمان نوبت ثبت خود، مقداری توکن سورن، بابت ثبت آن بلوک دریافت می‌کند. این مقدار توکن، پاداش ثبت بلوک نامیده می‌شود.
- کارمزد تراکنش: هر فرستنده‌ی تراکنش در زمان ارسال آن تراکنش به شبکه، باید مقداری توکن سورن بپردازد. توکن پرداختی تمام تراکنش‌های هر بلوک در زمان ثبت بلوک به حساب تأییدکننده‌ای که آن بلوک را ثبت می‌کند، واریز می‌شود.

۴-۲-۳-۳- روابط مالی صاحبان کسب‌وکارها

صاحبان کسب‌وکارها با طرف‌های زیر در تعامل هستند:

- هزینه‌هایی را که کاربران کسب‌وکارها طبق قواعد کسب‌وکار به حساب آنان واریز می‌کنند، دریافت می‌نمایند.
- جوایز یا پاداش‌ها یا موارد دیگری که طبق قواعد خود باید به کاربران بپردازند، پرداخت می‌نمایند.
- بابت توسعه‌های مربوط به اپلیکیشن‌ها و قراردادهای هوشمند، مبالغی را طبق تعهداتشان به توسعه‌دهنده‌ها پرداخت می‌کنند.
- توکن‌های دریافتی را توسط مراکز تبادل با توکن‌ها یا مبالغ لازم مبادله می‌کنند.

۴-۲-۳-۴- روابط مالی کاربران کسب‌وکارها

- کاربران کسب‌وکارها طبق قواعد هر کسب‌وکار مبالغی را در قالب توکن سورن یا توکن‌های دیگر شبکه به صاحبان کسب‌وکار پرداخت می‌کنند.
- کاربران ممکن است مبالغی را به عنوان پاداش یا جایزه از صاحبان کسب‌وکارها دریافت کنند.
- کاربران می‌توانند برای تهیه‌ی توکن‌های لازم به مراکز تبادل مراجعه کنند.

¹ Validator

۴-۲-۳-۵- روابط مالی مراکز تبادل

تمام طرف‌های درگیر در شبکه‌ی بلاکچین سور برای استفاده از توکن‌های سورن یا توکن‌های همسان و قابل مبادله، با مراجعه به یکی از سایت‌های مرکز تبادل، با پرداخت پول توکن مورد نیاز خود را تهیه می‌کنند.

همچنین در صورتی که توکنی را در اختیار داشته باشند و بخواهند آن را به فروش برسانند، به مراکز تبادل مراجعه می‌کنند.

در ازای این خدمات، سایت مرکز تبادل درصد کوچکی از توکن‌های مبادله شده را به عنوان کارمزد از فروشنده و خریدار دریافت می‌کند. این درصد طبق سیاست‌های هر سایت مرکز تبادل تعیین می‌شود.

۴-۲-۳-۶- روابط مالی توسعه‌دهنده‌ها

توسعه‌دهنده‌ها به ازای خدماتی که برای طرف‌های مختلف شبکه‌ی بلاکچین سور انجام می‌دهند، مزد کار خود را دریافت می‌کنند.

۴-۲-۴- کارمزد تراکنش

۴-۲-۴-۱- هزینه‌ی تراکنش بر حسب سوخت

سوخت (یا گس^۱) در بلاکچین سور، مقدار کمی از توکن سورن است که با استفاده از آن کارمزد تراکنش‌ها پرداخت می‌شود. کارمزد تراکنش‌ها بر حسب واحد سوخت به طور خودکار تعیین می‌شود. مقدار سوخت لازم برای هر تراکنش بستگی به نوع تراکنش و مقدار پردازش لازم برای انجام تراکنش و نیز ظرفیت ذخیره‌سازی لازم برای آن تراکنش دارد. مثلاً تراکنش پرداخت سورن از یک حساب به حساب دیگر به طور ثابت به میزان ۲۱۰۰۰ سوخت می‌باشد.

۴-۲-۴-۲- قیمت سوخت بر حسب سورن

حال به این نکته بپردازیم که هر واحد سوخت چه ارتباطی با توکن پایه‌ی شبکه (سورن) دارد. به عبارت دیگر قیمت هر واحد سوخت چند سورن است؟

¹ Gas

در واقع ارسال کننده‌ی تراکنش، که هزینه‌ی تراکنش توسط وی پرداخت می‌شود، قیمت هر واحد سوخت را بر حسب سورن، تعیین می‌کند. اما باید به این نکته توجه داشت که هر تأییدکننده می‌تواند قیمت حداقل هر واحد سوخت جهت پذیرش تراکنش را برای خود تعیین کند. به عبارت دیگر اگر قیمت حداقل سوخت شبکه برای تأییدکننده از قیمت سوخت شبکه که توسط کاربر فرستنده‌ی تراکنش تعیین شده، بیشتر باشد، آن تأییدکننده تراکنش ارسال شده را تأیید نخواهد کرد و تصمیم برای تأیید تراکنش به تأییدکننده‌های دیگر خواهد رسید.^۱

۴-۲-۴-۳- هزینه‌ی تراکنش بر حسب ریال

اما هزینه‌ی تراکنش بر حسب واحد پول ریال چه مقدار است؟ هزینه‌ی تراکنش بر حسب ریال حاصل ضرب این سه عامل خواهد بود:

- هزینه‌ی تراکنش بر حسب سوخت (که به نوع تراکنش و مشخصات آن بستگی دارد)
- قیمت پیشنهادی سوخت بر حسب سورن (که به تأییدکننده‌ها بستگی دارد و در نهایت توسط فرستنده‌ی تراکنش انتخاب می‌شود).
- قیمت سورن بر حسب ریال (که به بازار عرضه و تقاضا بستگی دارد و در قسمت بعد در مورد آن صحبت می‌شود)^۲

^۱ فرض کنیم ۲۰ تأییدکننده در شبکه فعال هستند و تأییدکننده‌ی الف حداقل قیمت سوخت مربوط به خود را ۰,۱ میکروسورن (۰,۰۰۰۰۰۱ سورن) تعریف کرده است، در حالی که بقیه‌ی تأییدکننده‌ها حداقل قیمت سوخت خود را ۰,۳ میکروسورن تعریف کرده باشد. اگر کاربری برای تراکنش ارسالی خود مثلاً قیمت ۰,۳ میکروسورن یا بیشتر را تعریف کند، اولین تأییدکننده‌ای که با توجه به نوبت چرخشی شبکه نوبت او باشد، آن تراکنش را تأیید خواهد نمود. اما اگر کاربر برای تراکنش ارسالی خود عدد ۰,۲ میکروسورن را تعیین کند، هیچ تأییدکننده‌ای به جز الف آن تراکنش را تأیید نخواهد کرد و ممکن است برای رسیدن نوبت به الف، این کاربر مدتی منتظر تأیید تراکنش بماند. به این ترتیب هزینه‌ای که کاربر به ازای کم کردن قیمت سوخت می‌پردازد، دیر تأیید شدن تراکنش خواهد بود. اگر کاربر قیمت سوخت تراکنش خود را کمتر از ۰,۱ میکروسورن تعیین کند، آن تراکنش توسط هیچ یک از تأییدکننده‌ها تأیید نخواهد شد و تراکنش در صف تراکنش‌ها باقی خواهد ماند تا روزی که حداقل یکی از تأییدکننده‌ها حداقل قیمت سوخت خود را تا حد مورد نظر پایین آورد و یا کاربر ارسال کننده همان تراکنش را به قیمت سوخت بالاتر تغییر دهد.

^۲ به عنوان مثال فرض کنید یک کاربر می‌خواهد تعدادی توکن سورن را برای کاربر دیگر ارسال کند. این تراکنش ۲۱۰۰۰ واحد سوخت هزینه دارد. فرض کنید کمترین قیمت سوخت بین تأییدکننده‌ها ۰,۲ میکروسورن باشد و کاربر نیز همین قیمت را انتخاب کند. همچنین فرض کنید که قیمت هر سورن در بازار ده هزار ریال (۱۰۰۰ تومان) باشد. به این ترتیب هزینه‌ی این تراکنش برابر با $۲۱۰۰۰ \times ۰,۰۰۰۰۰۰۲ \times ۱۰۰۰۰$ یعنی ۴۲ ریال خواهد بود.

۴-۲-۵- نحوه‌ی پایدارسازی و تعیین قیمت توکن پایه‌ی شبکه

در شبکه‌ی بلاکچین سور، چندین عامل خودکار همراه با بعضی عوامل قابل تنظیم که در اختیار تأییدکننده‌ها است، باعث پایداری قیمت سورن (توکن پایه‌ی شبکه) می‌شود. در این قسمت به بررسی این عوامل می‌پردازیم:

بازار عرضه و تقاضا به خودی خود عامل پایداری قیمت کالا و خدمات است، البته به این شرط که بین عرضه و تقاضا یک تعادل نسبی وجود داشته باشد.^۱

تأییدکننده‌ها نیز جزئی از بازار عرضه و تقاضا هستند و پایداری بازار به نفع آنها است. هر تأییدکننده یک عامل قابل کنترل جهت تنظیم در اختیار دارد و آن تعیین «حداقل قیمت سوخت»^۲ است. با تنظیم این عامل آن تأییدکننده هیچ تراکنشی با قیمت سوخت کمتر از آن حداقل را ثبت نخواهد کرد. تعیین این عامل طی یک فرایند رقابتی موجب پایین آمدن «حداقل قیمت سوخت» بین تأییدکننده‌ها و در نهایت کم شدن هزینه‌ی کارمزد تراکنش‌ها برای کاربران نهایی سیستم خواهد شد.^۳

^۱ در یک بازار آزاد، تقاضای بیشتر از جانب مصرف‌کننده باعث افزایش قیمت می‌شود. این افزایش قیمت از یک سو موجب کم شدن تقاضا و در نتیجه پایداری شدن قیمت می‌شود و از سوی دیگر باعث ترغیب عرضه‌کننده به عرضه‌ی بیشتر و باز هم موجب پایداری شدن قیمت می‌گردد.

از بعد دیگر افزایش عرضه از جانب عرضه‌کننده سبب کاهش قیمت می‌شود. این کاهش قیمت نیز از یک سو موجب ترغیب مصرف‌کننده و در نتیجه بیشتر شدن تقاضا و پایداری قیمت می‌گردد و از سوی دیگر باعث کم شدن عرضه و باز هم پایداری قیمت می‌شود.

^۲ Minimum Gas Price

^۳ اگر یک تأییدکننده در رقابت با سایر تأییدکننده‌ها حداقل قیمت سوخت خود را کم کند، منجر به این خواهد شد که سهم او از تأیید تراکنش‌ها و در نهایت سهم او از هزینه‌ی تراکنش‌ها بیش از سایر تأییدکننده‌ها خواهد شد، ولی به نسبت قیمت سوخت کمتر که این کم شدن قیمت با تعداد بیشتر تراکنش‌ها جبران خواهد گردید. این موضوع سایر تأییدکننده‌ها را نیز ترغیب خواهد نمود تا آنها نیز حداقل قیمت سوخت خود را کم کنند. اما این موضوعی نیست که تا ابد قابل تداوم باشد. قیمت سوخت تا جایی می‌تواند کم شود که هزینه‌های مربوط به تأییدکننده‌ها را پوشش دهد و مقداری سود نیز برای تأییدکننده‌ها به همراه داشته باشد. تعیین قیمت کمتر برای حداقل قیمت سوخت منجر به زیان تأییدکننده‌ها خواهد شد و آنان نمی‌توانند این مسابقه را در زمان طولانی ادامه دهند.

اگر قیمت سورن به ریال در بازار عرضه و تقاضا زیاد شود، درآمد تأییدکننده‌ها به همان نسبت بیشتر می‌شود و تأییدکننده‌ها قابلیت رقابت بیشتری با یکدیگر پیدا خواهند کرد تا برای افزایش سهم خود از بازار حداقل قیمت سوخت را کم کنند و این موضوع به پایداری قیمت سوخت نسبت به ریال منجر خواهد شد.

اگر هزینه‌های تأییدکننده‌ها مانند هزینه‌ی نگهداری سرور و ... زیاد شود، آنان ناگزیر خواهند بود، برای ادامه‌ی خدمات رسانی حداقل قیمت سوخت را افزایش دهند. این منجر به افزایش هزینه‌ی تراکنش‌ها تا حد پایداری دیگر

۴-۳- کاربرد سور

هدف نهایی در شبکه‌ی بلاکچین سور پیاده‌سازی قراردادهای هوشمند و نیز اجرای آن بر بستر این شبکه است.

انواع تراکنش‌های شبکه‌ی بلاکچین سور شامل موارد زیر می‌شود:

۱- پیاده‌سازی قرارداد هوشمند

۲- اجرای یک تابع از یک قرارداد هوشمند (و امکان ارسال توکن شبکه همراه آن)

۳- ارسال توکن سورن از یک حساب به یک حساب دیگر

بنابراین شبکه‌ی سور برای پیاده‌سازی قراردادهای هوشمند مربوط به فعالیت‌های اقتصادی و نیز غیرانتفاعی سازمان‌های بزرگ، شرکت‌ها، استارت‌آپ‌ها و مؤسسات غیر انتفاعی که بخواهند از مزایای بلاکچین در امور خود بهره‌مند شوند، قابل استفاده است.

۴-۴- نحوه‌ی تولید توکن سورن

در بلوک ابتدایی^۱ بلاکچین سور تعداد ۲۰ میلیون توکن سورن تولید می‌شود. همچنین در زمان ساخت هر بلوک تعدادی توکن نیز تولید می‌شود. تعداد توکن‌های تولید شده در هر بلوک به مرور زمان کاهش می‌یابد تا تعداد توکن‌های تولید شده در نهایت تعداد ثابت ۲۰۰ میلیون توکن پس از حدود ۲۰ سال باشد. بنا بر این است که در هر ۲ ثانیه یک بلوک جدید تشکیل شود. بعد از هر ۱۵ میلیون بلوک دوره‌ی زمانی جدیدی برای بلاکچین آغاز می‌شود و پاداش بلوک تغییر می‌یابد. هر دوره‌ی زمانی حدود یک سال به طول می‌انجامد.

رویه‌ی تولید توکن به عنوان پاداش بلوک در طی ۲۰ دوره‌ی اول در جدول ۷ آمده است.

به این ترتیب پس از ۲۰ دوره (یا حدود ۲۰ سال) و تولید ۳۰۰ میلیون بلوک، پاداش ثبت بلوک به صفر خواهد رسید. تا آن زمان ۲۰۰ میلیون توکن در شبکه تولید خواهد شد.

خواهد شد. ناگفته پیداست که این شرایط در زمان تورم به وقوع خواهد پیوست و افزایش هزینه‌ی تراکنش‌ها به نسبت تورم عمومی جامعه موضوعی اجتناب‌ناپذیر خواهد بود.

¹ Genesis Block

نمودار تعداد توکن تولیدی در طی ۲۰ دوره‌ی اول در شکل ۴ نمایش داده شده است. همچنین نمودار تجمعی تعداد توکن‌های سورن تولیدی در طی همین دوره‌ها در شکل ۵ آمده است.

جدول ۷- رویه‌ی تولید توکن به عنوان پاداش ثبت بلوک در طی ۲۰ دوره‌ی اول

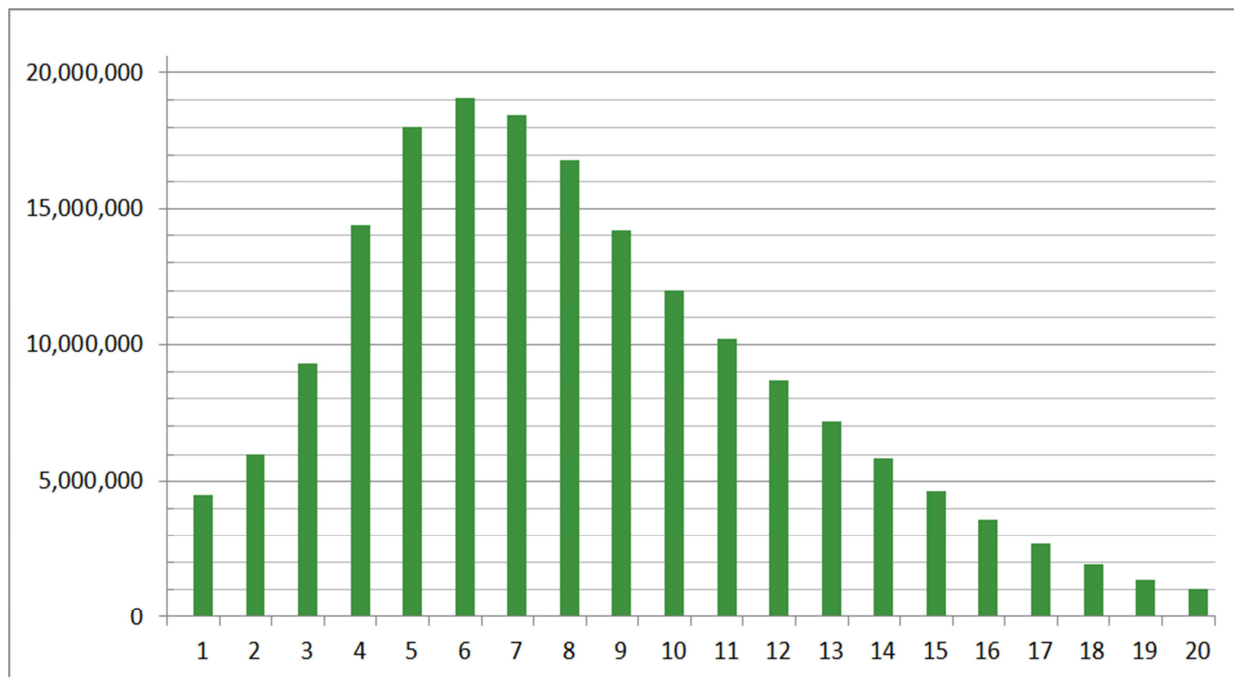
دوره	پاداش بلوک (سورن)	تعداد توکن تولیدی در طی دوره	دوره	پاداش بلوک (سورن)	تعداد توکن تولیدی در طی دوره
۱	0.30	4,500,000	۱۱	0.68	10,200,000
۲	0.40	6,000,000	۱۲	0.58	8,700,000
۳	0.62	9,300,000	۱۳	0.48	7,200,000
۴	0.96	14,400,000	۱۴	0.39	5,850,000
۵	1.20	18,000,000	۱۵	0.31	4,650,000
۶	1.27	19,050,000	۱۶	0.24	3,600,000
۷	1.23	18,450,000	۱۷	0.18	2,700,000
۸	1.12	16,800,000	۱۸	0.13	1,950,000
۹	0.95	14,250,000	۱۹	0.09	1,350,000
۱۰	0.80	12,000,000	۲۰	0.07	1,050,000

۴-۵- نحوه‌ی توزیع توکن سورن

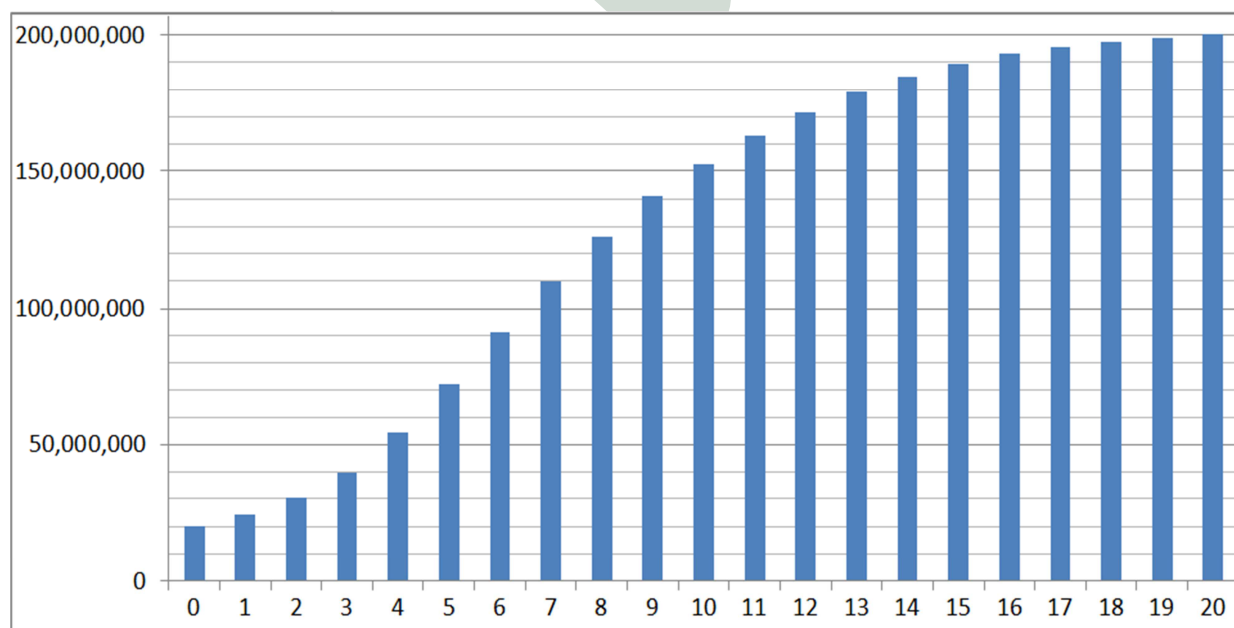
در بلوک ابتدایی بلاکچین سور^۱ تعداد ۲۰ میلیون توکن سورن تولید می‌شود. از این تعداد توکن ۱۰ میلیون توکن طی یک برنامه‌ی عرضه‌ی اولیه‌ی خصوصی به فروش خواهد رسید. قیمت پیش‌فروش توکن برابر یک ده‌هزارم توکن اتر در شبکه‌ی اتریوم خواهد بود.^۲

^۱ Genesis Block

^۲ در زمان انتشار این نگارش سپیدنامه این قیمت حدود ۵,۰۰۰ ریال است.



شکل ۴- نمودار تولید توکن سورن طی بیست سال ابتدایی راه‌اندازی شبکه



شکل ۵- نمودار تجمعی تولید توکن سورن طی بیست سال ابتدایی راه‌اندازی شبکه

باقیمانده‌ی توکن‌های تولیدشده‌ی اولیه^۱ در بلوک ابتدایی بلاکچین سور، برابر با ۱۰ میلیون توکن در یک کیف توکن چند امضایی^۲ که تحت یک قرارداد هوشمند برای بنیاد سور ایجاد می‌شود، ذخیره می‌گردد تا برای صرف هزینه‌های بنیاد خرج شود. این قرارداد هوشمند تنها با پیشنهاد یکی از اعضای بنیاد و قبول حداقل دو سوم اعضا می‌تواند مبالغ موجود در حساب را هزینه کند.

علاوه بر این در هر بلوک پاداش بلوک^۳ نیز تولید می‌شود. پاداش بلوک تولید شده به ترتیب زیر توزیع می‌شود:

- ۹۰٪ از پاداش بلوک تولیدشده به حساب تأییدکننده‌ی بلوک واریز می‌شود.
- ۱۰٪ از پاداش بلوک تولیدشده به حساب بنیاد واریز می‌شود تا برای هزینه‌های لازم بنیاد صرف شود.

۴-۶- درآمدهای بنیاد سور

درآمدهای بنیاد سور از محل‌های زیر تأمین خواهد شد:

- عرضه‌ی اولیه‌ی خصوصی ۱۰ میلیون توکن سورن (نیمی از توکن‌های تولیدشده در بلوک پیدایش)
- استفاده از ۱۰ میلیون توکن که در اختیار بنیاد قرار گرفته است (نیم دیگر توکن‌های تولیدشده در بلوک پیدایش)
- استفاده از ۱۰٪ از درآمد تأییدکننده‌های شبکه که به طور خودکار در اختیار بنیاد قرار می‌گیرد.
- استفاده از کمک‌های نهادهای دولتی و مردمی

۴-۷- هزینه‌های بنیاد سور

هزینه‌های بنیاد سور و درصد آن نسبت به درآمدهای محقق‌شده‌ی بنیاد در طی ۱۰ سال اول فعالیت شامل این موارد خواهد بود:

^۱ Pre-mined Tokens

^۲ Multi-signature Wallet

^۳ Block Reward

- هزینه‌ی توسعه‌ی نرم‌افزاری هسته‌ی اولیه‌ی بلاکچین و سیستم‌های وابسته: ۲۵٪ از درآمد بنیاد
 - هزینه‌ی دستمزد اعضای بنیاد: ۱۵٪ از درآمد بنیاد
 - توزیع رایگان توکن سورن به کاربران و اپلیکیشن‌ها و واگذاری به تعدادی از دانشگاه‌های کشور برای توسعه، آموزش، ترویج و تأمین سرور: ۲۰٪ از درآمد بنیاد
 - هزینه‌ی تبلیغات و رسانه‌ها: ۱۰٪ از درآمد بنیاد
 - هزینه‌ی تولید محتوا، آموزش و ترویج: ۱۵٪ از درآمد بنیاد
 - هزینه‌ی برگزاری سمینارهای سالانه: ۵٪ از درآمد بنیاد
 - هزینه‌های پیش‌بینی‌نشده: ۱۰٪ از درآمد بنیاد
- قیمت‌های فوق بر اساس قیمت‌های موجود در زمان تألیف سپیدنامه در سال ۱۳۹۹ برآورد شده است و از آن جا که توکن سورن به مرور زمان طبق بازار عرضه و تقاضا با وضع اقتصادی جامعه تطبیق پیدا خواهد کرد، و این توکن منبع تهیه‌ی اعتبار برای انجام هزینه‌ها خواهد بود، خودبه‌خود مقدار اعتبار برای هزینه‌ها در سال‌های بعد، خود را با قیمت‌های آینده منطبق خواهد نمود.
- نهاد حساب‌رسی در بنیاد سور وظیفه‌ی نظارت بر درآمدها و هزینه‌های بنیاد و انطباق آن با مصوبات را بر عهده دارد.

۴-۸- طرح بازاریابی برای پلتفرم سور

منظور از بازاریابی پلتفرم سور جذب افراد کارآفرین، کسب‌وکارها، شرکت‌ها و سازمان‌های مختلف برای توسعه‌ی اپلیکیشن‌های بلاکچینی خود روی پلتفرم سور است. علاوه بر آن هر کسب‌وکار خود متولی تبلیغات خود برای جذب مخاطب می‌باشد. اما بنیاد سور نیز برای کمک به کسب‌وکارها برای جذب مخاطب نیز طرح‌هایی در پیش رو دارد:

- به تعدادی از دپ‌های کاربردی اولیه با معیارهای مناسب طبق آیین‌نامه‌ی مصوب بنیاد، تعدادی توکن سورن تعلق می‌گیرد تا با نظارت بنیاد بین اولین کاربران خود توزیع نمایند. به این ترتیب در تأمین هزینه‌ی بازاریابی کمک قابل توجهی به کسب‌وکارهای اولیه بر روی این بلاکچین انجام می‌شود.

- بنیاد سور به تعدادی از نخستین کاربرانی که آدرس کیف توکن خود و معرف خود را ثبت کنند، تعدادی توکن به خود فرد و معرفش واریز می‌کند تا در مبادلات خود از آن استفاده کنند.
- برای جذب مخاطبان به شبکه‌ی سور می‌توان از انواع روش‌های برگزاری کمپین‌های تبلیغاتی، برگزاری دوره‌های آموزشی، سمینارها، تهیه‌ی فیلم و مانند آن استفاده کرد.

۴-۹- حدود مسئولیت‌ها

- یکی از مواردی که باید در راه اندازی این پلتفرم مورد بررسی قرار گیرد، حدود مسئولیت ذینفعان مختلف پلتفرم بلاکچین سور است. این موضوع باید از دیدگاه‌های مختلفی مورد بررسی قرار گیرد:
- **بنیاد سور و تأییدکننده‌ها:** از دیدگاه فنی امکان کنترل کسب‌وکارها و اپلیکیشن‌هایی که به عنوان بستر بلاکچین از پلتفرم سور استفاده می‌کنند، وجود ندارد، بنابراین بنیاد سور و تأییدکننده‌ها نفیاً و اثباتاً امکان پذیرش هیچ گونه مسئولیتی در رابطه با کسب‌وکارها و اپلیکیشن‌ها را ندارند. اما بنیاد سور این با کمک تأییدکننده‌ها در حد توان خود با مراجع قضایی همکاری لازم را مبذول خواهند داشت و در عین حال مالکیت یا مسئولیت دیگری نسبت به محتوای قانونی کسب‌وکار ندارند.
- **توسعه‌دهندگان:** توسعه‌دهندگان محتوا در شبکه‌ی بلاکچین سور هویت حقوقی ندارند. از این رو هر فردی به طور جداگانه مسئول محتوای خود است. به عنوان مثال اگر توسعه‌دهنده‌ای به طور شخصی یا به سفارش یک کسب‌وکار اقدام به راه‌اندازی یک قرارداد هوشمند مبتنی بر پلتفرم بلاکچین سور نماید، خود مسئول اعمال خود است و فرد دیگری مسئول عمل وی محسوب نمی‌شود.
- **کاربران:** کاربران و استفاده‌کنندگان از اپلیکیشن‌های شبکه مسئول اعمال خود هستند. آنان نیز بنا بر تشخیص خود از برنامه‌های شبکه که توسط افراد دیگر ایجاد شده‌اند، استفاده می‌کنند. البته واضح است که مسئولیت کاربران یک برنامه نافی مسئولیت ایجاد کننده‌ی آن نمی‌باشد. کاربران اپلیکیشن‌ها و توکن‌های پلتفرم بلاکچین سور، باید مقررات و در صورت وجود سپیدنامه‌ی هر طرح را مطالعه کنند و با دید باز در آن مشارکت نمایند. بدیهی است که مسئولیت مشارکت یا فعالیت در یک طرح بر عهده‌ی خود کاربران است.

- **صاحبان کسب‌وکار:** مسئولیت صاحبان کسب‌وکارها در مورد ایجاد محتوا بر روی شبکه نیز عیناً مشابه مسئولیت مدیران و مؤسسان وب‌سایت‌ها در مورد ایجاد محتوای غیرقانونی بر روی سایت است. به این ترتیب صاحبان کسب‌وکارهای مبتنی بر شبکه‌ی بلاکچین سور مسئول نتایج کسب‌وکار خود و محتوای قراردادهای هوشمند خود می‌باشند.

فصل ۵- معرفی بنیاد سور

بنیاد سور مؤسسه‌ای در حال ثبت است که متشکل از افراد حقیقی و حقوقی مؤسس شبکه‌ی بلاکچین سور است که همگی در صنعت بلاکچین ایران در حال فعالیت هستند.

عضویت اعضای جدید در بنیاد سور در صورت تصویب حداقل دوسوم اعضای بنیاد و طی مراحل اداری لازم امکان‌پذیر است.

وظایف بنیاد سور طبق اساسنامه‌ی آن از قرار زیر است:

- طراحی و توسعه کد متن باز بلاکچین سور و به روز رسانی آن
 - راه‌اندازی اولیه‌ی بلاکچین سور
 - تبصره: بنیاد سور هیچ گونه مسئولیتی در رابطه با کسب‌وکارهای فعال بر بستر سور ندارد و هریک از فعالان بایستی بر اساس شرایط و قوانین کشور مجوزهای لازم را از مراجع مربوطه دریافت نمایند.
 - سازماندهی تأیید کنندگان اولیه و تلاش جهت توسعه‌ی شبکه‌ی تأیید کنندگان
 - جلب مشارکت فعالان صنعت بلاکچین و رایزنی برای توسعه و به روز رسانی بلاکچین سور
 - برگزاری گردهمایی سالانه فعالان و توسعه‌دهندگان بلاکچین سور
 - تدوین متن توافقنامه بین بنیاد و کاربران شبکه بلاکچین سور موسوم به سپیدنامه
 - توزیع توکن‌های پایه‌ی شبکه (سورن) که در بلاک پیدایش شبکه تولید شده‌اند، بر مبنای سپیدنامه
 - فعالیتهای آموزشی و ترویجی در جهت توسعه کاربری بلاکچین سور
- بنیاد برای امور توسعه پس از فراخوان و دریافت پیشنهادها طی یگ فرآیند رقابتی و شفاف که آیین‌نامه‌ی آن متعاقباً اعلام خواهد شد مناسب‌ترین کارفرما را انتخاب خواهد کرد.

فصل ۶- نقشه‌ی راه

راه اندازی و تداوم راه پلتفرم بلاکچین سور در این گام‌ها پیش‌بینی شده است:

- نگارش سپیدنامه
- نگارش اساس‌نامه
- ثبت قانونی بنیاد سور به عنوان مؤسسه‌ی غیرتجاری
- توسعه‌ی فنی پلتفرم اولیه
- راه‌اندازی وب سایت بنیاد سور
- مشخص شدن نهایی تأییدکننده‌های اولیه (از بنیاد سور و خارج از بنیاد سور)
- پیش راه اندازی و تست
- راه‌اندازی اولیه‌ی پلتفرم بلاکچین سور
- ایجاد زیرساخت حقوقی فعالیت
- فراخوان جذب سرمایه گذاران خصوصی
- برگزاری فراخوان پیمانکار توسعه از طرف بنیاد
- توسعه‌ی سرویس‌های اولیه جهت استفاده از بلاکچین سور
- شروع کمپین‌های آموزشی و تبلیغی با هدف توسعه بازار
- تبلیغ جهت جذب کاربران اولیه
- دستیابی به اهداف فاز اول توسعه‌ی بازار
- توسعه‌ی تعداد تأییدکننده‌ها
- توسعه‌ی شرکای راهبردی نظیر دانشگاه‌ها و مراکز آموزشی و پژوهشی
- اعلان جهت راه‌اندازی محیط‌های جانبی مانند اکسپلورر و تبادل توکن با واحد پول

- اعلان جهت جذب همکاری سازمان‌ها و بانک‌ها
- توسعه زیرساخت تعاملات بین شبکه‌ای

دفتر
فصل
انتشار

فصل ۷ – جمع‌بندی

پلتفرم بلاکچین سور با هدف ارائه‌ی یک بستر مطمئن، ارزان و محرمانه برای پیاده‌سازی اپلیکیشن‌های توزیع‌شده بر بستر قراردادهای هوشمند راه‌اندازی شده است. در این پلتفرم بنیاد سور با همکاری تأییدکننده‌ها، توسعه‌دهندگان، صاحبان کسب‌وکارها و کاربردهای مبتنی بر بلاکچین، مراکز تبادل و کاربران اپلیکیشن‌ها در یک بستر بر مبنای قوانین کشور و نیز قواعد پذیرفته‌شده به تعامل با یکدیگر می‌پردازند و امور دیگران را در کنار اصلاح امور خود تسهیل می‌نمایند.

پیوست ۱ – نقشه‌ی راه توسعه‌ی نرم‌افزاری بلاکچین سور

نقشه‌ی راه پیش رو برای توسعه‌ی بلاکچین سور در دو موضوع مورد بررسی قرار می‌گیرد:

- توسعه‌های نرم‌افزاری لازم برای یک شبکه‌ی بلاکچین قراردادهای هوشمند عمومی. این اجزا در این ضمیمه مورد بررسی قرار خواهند گرفت.
- توسعه‌های نرم‌افزاری که در طول مسیر نیاز به آنها مشخص می‌شود. در این ضمیمه روش اجماع در مورد آنها مورد بررسی قرار خواهد گرفت.

پ ۱-۱ – توسعه‌ی نرم‌افزاری اولیه

در طول مسیر ساخت یک بلاکچین برای پیاده‌سازی قراردادهای هوشمند لازم است که بعضی توسعه‌های نرم‌افزاری هم در سطح سرویس‌دهنده‌ها و هم در سطح کاربران صورت گیرد. اهم این موارد را می‌توان به این ترتیب فهرست نمود:

در سطح سرویس‌دهنده‌ها:

- هسته‌ی اصلی شبکه
- مرورگر شبکه یا اکسپلورر^۱
- سرورهای ارائه‌دهنده‌ی خدمات ارتباط با شبکه (مانند اینفورا در شبکه‌ی اتریوم)
- نمایشگر شبکه^۲
- ساخت و آپلود ایمیج‌های داکر^۳
- تهیه‌ی وب‌سایت بنیاد سور با همه‌ی اجزای لازم

^۱ Explorer

^۲ Network Monitor

^۳ Docker

- تهیه‌ی یک انجمن گفتگو همراه با اجزای خاص لازم مانند امکان اتصال به بلاکچین سور جهت رأی‌گیری و ...

در سطح کاربران:

- والت به عنوان اکستنشن برای مرورگرها (مانند متامسک در شبکه‌ی اتریوم)
- والت دسکتاپ برای سیستم عامل‌های ویندوز، لینوکس و مک
- والت مبتنی بر وب (مانند مای‌اترولت در شبکه‌ی اتریوم)
- والت فول‌نود
- والت لایت‌نود
- والت موبایل برای سیستم عامل‌های اندروید و آی‌اواس

علاوه بر این موارد، تهیه‌ی مستندات فنی برای این فرآیندها لازم به نظر می‌رسد:

- هسته‌ی اصلی سرورهای تأییدکننده^۱
- نصب نگهداری و رفع مشکلات سرورهای تأییدکننده
- نصب فول‌نود و لایت‌نود

پ ۱-۲- توسعه‌ی نرم‌افزاری طبق نیازهای آتی

در مسیر پیشرفت بلاکچین سور لازم است که اعضای جامعه‌ی استفاده‌کنندگان از این شبکه با یکدیگر در ارتباط باشند. این ارتباط از طریق بعضی انجمن‌ها و تالارهای گفتگو در فضای انجمن‌های گفتگوی اختصاصی بنیاد انجام می‌شود. در فضای گفتگوی به وجود آمده به تدریج نیازهای جدید مشخص می‌شود، استانداردهای جدید ساخته می‌شود و هر جا که پس از ارائه‌ی نظرات مختلف یاز به رأی‌گیری از اعضای جامعه بود، بتوان با استفاده از یک رأی‌گیری مبتنی بر بلاکچین، به اجماع نسبی رسید.

مشروح این فرآیند به این ترتیب است:

¹ Validator

- افرادی که در طی بحث‌ها یا به صورت منفرد به پیشنهادی جهت بهبود کار بلاکچین برسند، پیشنهاد خود را به عنوان یک سند^۱ SIP در سیستم ثبت می‌کنند.
- اسناد SIP که در سیستم ثبت شده‌اند در انجمن‌های گفت‌وگوی مربوط به شور گذاشته می‌شوند. در طی این مباحث ممکن است پیشنهادها رد شوند، یا به تصویب برسند و یا بهبود داده شوند. در هر صورت در نهایت پیشنهادهاى نهایی به رأی گذاشته می‌شوند و در صورت آوردن رأی لازم، یک سند^۲ SRC تولید می‌شود.
- اگر سند SRC تولید شده حاوی یک استاندارد یا روش توسعه باشد، در همین مرحله به عنوان توصیه‌ی ثبت شده محفوظ می‌ماند و اعضای جامعه می‌توانند از آن استفاده نمایند.
- اگر سند SRC تولید شده حاوی پیشنهادی برای اجرا روی پلتفرم شبکه باشد، با هدایت بنیاد و طی مراحل لازم که در آیین‌نامه‌های بنیاد مشخص خواهد شد، پیمانکار لازم برای اجرای آن تعیین می‌شود و فرآیند مشخص شده توسعه داده می‌شود.

^۱ SIP: Sur Improvement Proposal

^۲ SRC: Sur Request for Comment

پیوست ۲- معرفی هایپرلجر بسو

هایپرلجر^۱ بسو اولین پروژه‌ی بلاکچین عمومی است که به طور رسمی به کنسرسیوم هایپرلجر پیوسته است. تا قبل از آن تنها پروژه‌های بلاکچین خصوصی به کنسرسیوم پیوسته بودند.

این پروژه قبل از پیوستن به هایپرلجر به نام پانتئون^۲ شناخته می‌شد. پذیرش این عضو جدید در تاریخ ۸ آگوست ۲۰۱۹ به کنسرسیوم پیشنهاد شد و در تاریخ ۲۹ آگوست ۲۰۱۹ رسماً اعلام شد که پروژه‌ی هایپرلجر بسو بخشی از کنسرسیوم خواهد بود.

هایپرلجر بسو یک پیاده‌سازی متن‌باز از اتریوم است که با مجوز آپاچی ۲٫۰ ایجاد شده‌است. این برنامه به زبان جاوا نوشته شده‌است و از شبکه‌ی عمومی اتریوم استفاده می‌کند.

یک پیاده‌سازی اتریوم نرم‌افزاری است که برای اجرا کردن پروتکل اتریوم به کار می‌رود. به عبارت دیگر این نرم‌افزار برای انجام موارد زیر به کار می‌رود:

- ایجاد یک محیط اجرایی در بلاکچین اتریوم برای پردازش تراکنش‌ها
 - ذخیره‌ی اطلاعات پایدار شامل ذخیره‌سازی نتایج اجرای تراکنش‌ها
 - به کار انداختن ارتباط شبکه هم‌تا به هم‌تا بین گره‌ها
 - ارائه‌ی API ها برای توسعه‌ی ایمن و تعامل با بلاکچین
- حال کمی به امکانات موجود در هایپرلجر بسو می‌پردازیم:

اولین چیزی که در مورد هایپرلجر بسو جلب توجه می‌کند، رابط خط فرمان آن است. همچنین API JSON-RPC را ارائه می‌دهد. هر دوی اینها می‌توانند برای پایش، عیب‌یابی، نگهداری، و اجرا در شبکه‌ی Ethereum استفاده شوند.

به طور خلاصه می‌توان از آن برای چیزهایی استفاده کرد که بسیار شبیه به چیزی هستند که شبکه‌ی اتریوم قادر به آن است:

^۱ Hyperledger BESU

^۲ Pantheon

● توسعه‌ی اپلیکیشن‌های کاربردی غیرمتمرکز یا DAPP^۱

● توسعه‌ی قرارداد هوشمند

● تولید توکن جدید

در هایپرلجربسو ابزارهای مشترک برای توسعه‌ی قراردادهای هوشمند و اپلیکیشن‌های غیرمتمرکز مانند Remix و Truffle و web3j ارائه می‌شود. شبکه‌ی هایپرلجربسو برای نیازهای سازمانی و فضای کسب‌وکار ایده‌آل است و موارد بسیاری از این نوع استفاده در حال حاضر در جریان است.

در هسته‌ی هایپرلجربسو یک ماشین مجازی اتریوم^۲ قرار گرفته است تا با استفاده از یک سیستم تورینگ کامل، برنامه‌های قراردادهای هوشمند را از طریق تراکنش‌های بلاکچینی اجرا کند.

هنگامی که سراغ متد اجماع برویم، این شبکه از متدهای اجماع اثبات اقتدار^۳ (با روش Clique و IBFT-2) و اثبات کار (با الگوریتم هش Ethash) استفاده می‌کند.

اثبات اقتدار برای زمانی مناسب است که نوعی اعتماد ایجاد شده بین نودهای شرکت‌کننده در اجماع شبکه وجود داشته باشد. این روش برای سازمان‌ها و کسب‌وکارها ایده‌آل است.

● برای رسیدن به اجماع می‌توان از روش IBFT-2 استفاده کرد. برای این کار وجود تعدادی حساب که هویت صاحبان آن مشخص باشد، لازم است. هر یک از حساب‌ها به عنوان یک ولیدیتور^۴ یا تأییدکننده برای مراقبت از بلوک‌ها و اعتبارسنجی تراکنش‌ها استفاده می‌شوند. سپس گروهی از تأییدکننده‌ها به عنوان یک نهاد قدرت عمل می‌کنند که در آن می‌توانند برای اضافه کردن یا حذف تأییدکننده‌های دیگر رأی‌گیری کنند. به این ترتیب در روش IBFT-2 هر کسی اجازه ندارد به سیستم اعتبارسنجی تراکنش‌ها و ثبت بلوک‌ها وارد شود و همیشه یک زنجیره‌ی اصلی برای این منظور وجود خواهد داشت. در این روش وجود حداقل دوسوم از تأییدکننده‌ها برای ثبت بلوک در شبکه لازم است.

● Clique یک الگوریتم حفاظتی است که تحمل‌پذیری مقداری از خطا را تضمین می‌کند. در این روش با خطای حداکثر نیمی از تأییدکننده‌ها شبکه می‌تواند به کار خود ادامه دهد.

^۱ DAPP: Decentralized Application

^۲ EVM: Ethereum Virtual Machine

^۳ POA: Proof Of Authority

^۴ Validator

هایپرلجربسو دارای API‌های بسیار عالی است. این API‌ها که برای ارتباط از پروتکل HTTP و WebSocket استفاده می‌کنند شامل EEA JSON-RPC و همچنین API‌های مربوط به شبکه‌ی اصلی اتریوم می‌باشد و از GraphQL API نیز پشتیبانی می‌کند.

بلاکچین هایپرلجربسو از پایش مشخصه‌های نظارتی، از جمله پایش شبکه و نمایشگر عملکرد نود پشتیبانی می‌کند. برنامه‌ی پرومتئوس^۱ برای پایش عملکرد گره‌ها مورد استفاده قرار می‌گیرد. همچنین از روش JSON-RPC API می‌توان برای اشکال‌زدایی استفاده کرد. برای پایش عملکرد شبکه نیز ابزارهای Alethi شامل مانیتور شبکه و EthStats یا بلاک اکسپلورر استفاده می‌شوند.

برای حفظ حریم خصوصی، هایپرلجربسو یک سیستم مدیریت تراکنش‌های خصوصی^۲ ارائه می‌دهد. این سیستم تضمین می‌کند که طرف‌های درگیر در یک تراکنش نباید نگران سرقت هویت یا هر گونه نشت اطلاعات باشند.

معماری هایپرلجربسو ساده و اثربخش است. اجزای کلیدی این معماری در نمودار شکل ۶ آمده‌اند و در این قسمت در مورد آن توضیح می‌دهیم:

سه مؤلفه‌ی اصلی هایپرلجربسو شامل موارد زیر است:

● ذخیره‌سازی^۳

● هسته‌ی اتریوم^۴

● شبکه‌سازی^۵

ابتدا در مورد هسته‌ی اتریوم بحث می‌کنیم. هسته متشکل از ماشین مجازی اتریوم^۶ است. وظیفه‌ی این ماشین مجازی اجرای هر تراکنش است. در قسمت بالایی ماشین مجازی اتریوم، پردازنده‌ی تراکنش‌ها^۷ قرار گرفته است که به عملکرد مؤثر و کارآمد این ماشین مجازی کمک می‌کند.

^۱ Prometheus

^۲ Private Transaction Manager

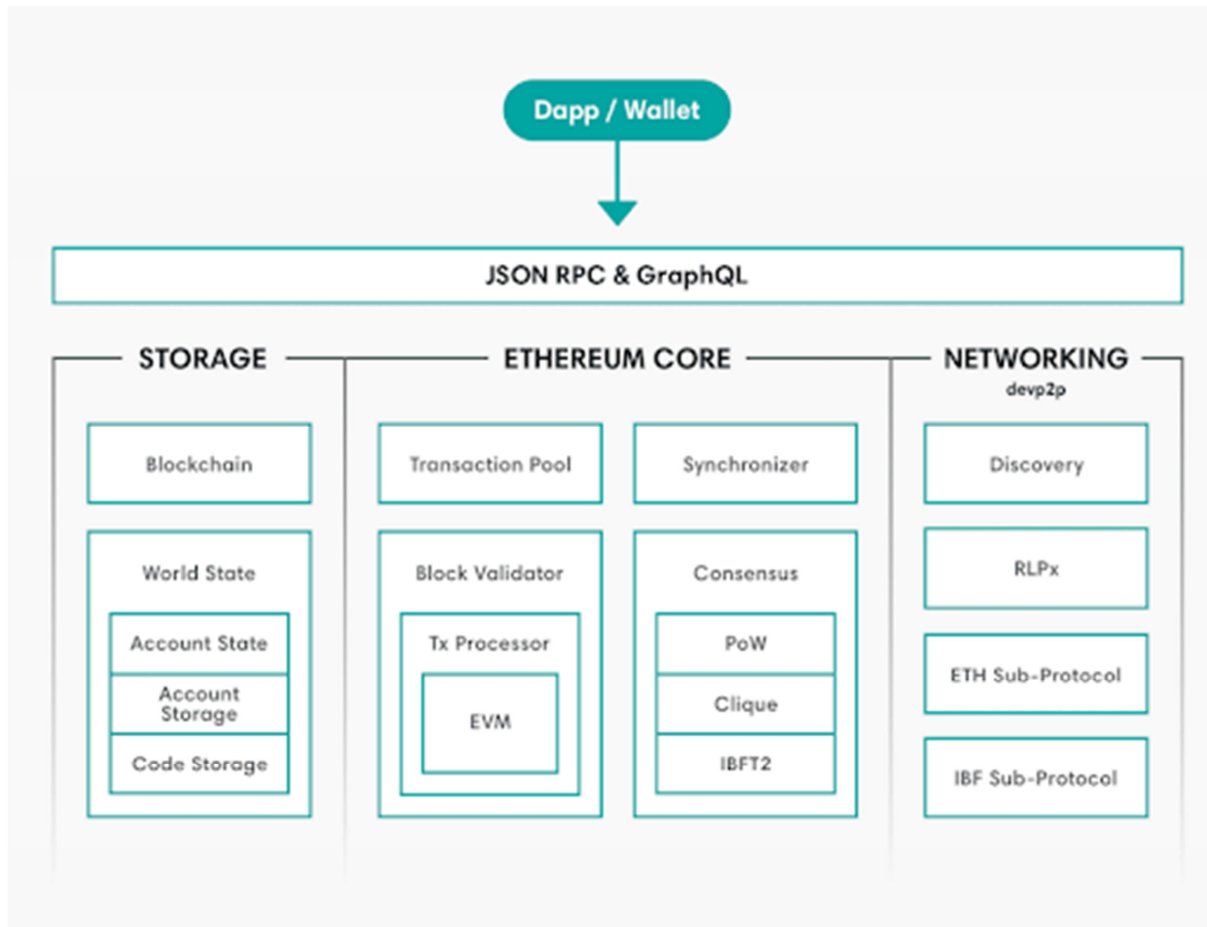
^۳ Storage

^۴ Ethereum Core

^۵ Networking

^۶ EVM: Ethereum Virtual Machine

^۷ Tx Processor



شکل ۶- معماری فنی هایرلجریسو

روش‌های اجماع^۱ نیز قسمتی از هسته‌ی اتریوم هستند.

دو جزء اصلی دیگر از هسته‌ی اتریوم عبارتند از:

- استخر تراکنش‌ها: اطلاعات تراکنش‌های ثبت‌نشده در بلاکچین را ذخیره می‌کند.

- همگام‌کننده^۲: به همگام‌سازی تمام گره‌ها در شبکه کمک می‌کند.

قسمت ذخیره‌سازی نیز شامل بلاکچین و وضعیت دنیای بیرون^۳ است. وضعیت دنیای بیرون نیز شامل

وضعیت حساب، ذخیره‌سازی حساب و ذخیره‌سازی کد برنامه می‌باشد.

^۱ Consensus

^۲ Synchronizer

^۳ World State

در نهایت نیز شبکه‌سازی هایپرلجربسو وجود دارد که با استفاده از پروتکل Ethereum devp2p کار می‌کند. چهار مؤلفه‌ی اصلی آن نیز عبارتند از:

- کشف
- RLPx
- زیرپروتکل ETH
- زیرپروتکل IBF

اعطای مجوز^۱ بخش مهمی از هر چارچوب بلاکچین سازمانی از جمله هایپرلجربسو است. هر شبکه‌ی قابل مجوزدهی^۲ حول این ایده شکل گرفته است که تنها به گره‌های خاص اجازه‌ی شرکت در شبکه می‌دهد. آن‌ها با انجام تراکنش یا اجازه‌ی ثبت دادن به تراکنش‌های دیگر، این شبکه را فعال می‌سازند و در آن شرکت می‌کنند.

در مورد یک شبکه‌ی هم‌تا به هم‌تا، لازم است که قواعد روی گره‌ها بررسی شود تا مجوزدهی قابل انجام شود. واضح است که در یک شبکه‌ی قابل مجوزدهی، پیش از اعطای مجوز به نودهای دیگر یک سطح اعتماد برای راه‌اندازی لازم است. برای اطمینان از اینکه بازیگران نادرست در اینجا فقط یک نقش حداقلی دارند، لازم است اقدامات احتیاطی انجام شود. به عنوان مثال، یک بازیگر نادرست نمی‌تواند بر تصمیم‌گیری در مورد شبکه تأثیر بگذارد. قوانین و مقررات مناسب می‌تواند به شناسایی فعالان نادرست و حذف آن‌ها در صورت شناسایی کمک کند.

علاوه بر اعطای مجوز به نودها، موضوع اعطای مجوز به حساب‌ها نیز وجود دارد که می‌تواند قوانین و مقررات بیشتری را اعمال می‌کند. اعطای مجوز به حساب‌ها را می‌توان برای اعمال الزامات هویت و دسترسی مورد استفاده قرار داد. همچنین به تعلیق حساب‌ها، لیست سیاه و محدود کردن حساب‌ها در هنگام لزوم کمک می‌کند.

^۱ Permissioning

^۲ Permissioned

فهرست

سپیدنامه بلاکچین سور	۲
فصل ۱- مقدمه	۳
فصل ۲- تعریف واژگان	۵
فصل ۳- زیرساخت‌های مشابه	۸
۱-۳- اتریوم	۸
۲-۳- ترون	۹
۳-۳- ای‌اواس	۱۰
۴-۳- کاردانو	۱۱
۵-۳- آلاستریا	۱۲
۶-۳- مقایسه‌ی زیرساخت‌های معرفی شده	۱۲
فصل ۴- معرفی پلتفرم سور	۱۴
۱-۴- معماری پلتفرم سور	۱۴
۱-۱-۴- مشخصات پلتفرم سور	۱۴
۲-۱-۴- اجماع در پلتفرم سور	۱۵
۳-۱-۴- جذب یا اخراج تأییدکنندگان	۱۵
۴-۱-۴- توکن پایه‌ی شبکه	۱۶
۵-۱-۴- مدل مفهومی پلتفرم سور	۱۶
۶-۱-۴- ذینفعان پلتفرم سور	۱۶

۲۰	۴-۱-۷- ارتباط داده‌ای بین ذینفعان.....
۲۱	۴-۲- اقتصاد بلاکچین سور.....
۲۲	۴-۲-۱- توکن پایه‌ی شبکه.....
۲۲	۴-۲-۲- توکن‌های قابل تعریف برای کسب‌وکارهای مختلف روی شبکه.....
۲۳	۴-۲-۳- ارتباط مالی طرف‌های مختلف شبکه با یکدیگر.....
۲۵	۴-۲-۴- کارمزد تراکنش.....
۲۷	۴-۲-۵- نحوه‌ی پایدارسازی و تعیین قیمت توکن پایه‌ی شبکه.....
۲۸	۴-۳- کاربرد سور.....
۲۸	۴-۴- نحوه‌ی تولید توکن سورن.....
۲۹	۴-۵- نحوه‌ی توزیع توکن سورن.....
۳۱	۴-۶- درآمدهای بنیاد سور.....
۳۱	۴-۷- هزینه‌های بنیاد سور.....
۳۲	۴-۸- طرح بازاریابی برای پلتفرم سور.....
۳۳	۴-۹- حدود مسئولیت‌ها.....
۳۵	فصل ۵- معرفی بنیاد سور.....
۳۶	فصل ۶- نقشه‌ی راه.....
۳۸	فصل ۷- جمع‌بندی.....
۳۹	پیوست ۱- نقشه‌ی راه توسعه‌ی نرم‌افزاری بلاکچین سور.....
۳۹	پ ۱-۱- توسعه‌ی نرم‌افزاری اولیه.....
۴۰	پ ۱-۲- توسعه‌ی نرم‌افزاری طبق نیازهای آتی.....
۴۲	پیوست ۲- معرفی هایپرلجربسو.....
۴۷	فهرست.....