**Stacks**

بیت کوین به عنوان اولین و بزرگ‌ترین رمز‌ارز در دنیا شناخته می‌شود. در شبکه بیت‌کوین برخی مشکلات و موانع وجود دارد که بسیاری از پروژه‌های بلاک‌چینی راهکارهایی برای رفع آن‌ها پیشنهاد کرده‌اند؛ یکی از محدودیت‌های قابل توجه شبکه Bitcoin، مشکلات ناشی از مقیاس‌پذیری آن است. استکس (Stacks) یکی از شبکه‌های لایه یک بلاکچینی است که تلاش می‌کند مشکلات مقیاس‌پذیری در شبکه بیت‌کوین را حل کند. همچنین استکس برای اجرای قراردادهای هوشمند و برنامه‌های غیر‌متمرکز (DApp) بر روی بلاک‌چین بیت کوین طراحی و اجرا شده است. هدف از راه‌اندازی این شبکه، امکان ایجاد ارتباط بین فن‌آوری‌های Blockchain با شبکه بیت کوین بدون نیاز به تغییر در این شبکه یا انجام فورک در آن است. **اما شبکه Stacks چیست؟**

استکس پلتفرمی است که استفاده از قرارداد‌های هوشمند و برنامه‌های غیر‌متمرکز را در شبکه بیت‌کوین تسهیل می‌بخشد. بلاک‌چین این شبکه برای حفظ امنیت و اجرای تراکنش‌ها، به بلاک چین بیت‌کوین وابسته است. به عبارت دیگر، شبکه بیت کوین به عنوان لایه نهایی و امنیتی، برای قرارداد‌های هوشمند و اجرا شده در بلاک‌چین استکس عمل می‌کند. این کار از طریق مکانیسم گواه اثبات انتقال (POX) Proof of Transferدر شبکه استکس انجام می‌شود.

ارتباط بین بلاک‌چین Stacks و بیت‌کوین، امکان اجرای تراکنش‌ها در شبکه استکس و تایید آنها در بلاک‌چین بیت‌کوین را فراهم می‌کند. انجام این کار باعث می‌شود امکان اجرای قرارداد‌های هوشمند روی شبکه بیت‌کوین توسط DApp های مختلف امکان‌پذیر شود؛ همچنین به دلیل اجرای تراکنش‌ها در شبکه استکس و تایید آن‌ها در بلاک‌چین بیت‌کوین، مشکل مقیاس‌پذیری در شبکه Bitcoin نیز تا حدود زیادی برطرف شود. این پلتفرم قبلا با نام Blockstack شناخته می‌شد، اما در پایان سال ۲۰۲۰ به Stacks تغییر نام داد تا این پروژه متن‌باز (Open Source) را از Blockstack PBC، شرکتی که به عنوان شرکت مادر آن است جدا کند.

این شبکه برای اجرای امن قراردادهای هوشمند، از زبان برنامه‌نویسی Clarity استفاده می‌کند. زبان برنامه‌نویسی Clarity یک زبان برنامه‌نویسی است که از کامپایلرها (Compiler) استفاده نمی‌کند و شبکه استکس این زبان برنامه‌نویسی را برای کمک به اسمارت کانترکت‌ها برای استفاده در شبکه بیت کوین به کار گرفته است؛ به طور دقیق‌تر، این زبان برنامه‌نویسی از کدهای منابع قابل پیش‌بینی برای اجرای قرارداد‌های هوشمند، در حین انتشار آن‌ها در نودهای بلاک‌چین استفاده می‌کند.

شبکه Stacks و Bitcoin دو شبکه بلاک‌چینی به هم پیوسته هستند که دست در دست هم کار می‌کنند. بسیار جالب است که این دو شبکه به هم وابسته نیستند؛ آن‌ها شبکه‌های مستقلی هستند که از طریق مکانیسم اجماع اثبات انتقال به هم متصل شده‌اند. از طریق این مکانیسم، ماینرها می‌توانند ارزهای دیجیتال جدید و قرارداد‌های هوشمند روی شبکه بیت کوین را به سایر افراد روی شبکه استکس منتقل کنند.

**هدف و ایده شبکه Stacks**

استکس یک شبکه بلاک‌چین لایه یک است که برای اضافه شدن Smart Contractها و DAPPها به شبکه بیت‌کوین طراحی شده است. این قراردادهای هوشمند، بدون تغییر در هیچ‌یک از ویژگی‌هایی که آن را بسیار قدرتمند می‌کند (مثل امنیت و ثبات)، شبکه به بیت‌کوین منتقل می‌شوند. برنامه‌های غیرمتمرکز ساخته شده بر روی شبکه Stacks متن‌باز هستند؛ به این معنی که توسعه‌دهندگان می‌توانند برنامه‌های یکدیگر را آپدیت کنند و آن‌ها را بهبود ببخشند و از آن‌جایی که استکس از بیت‌کوین به عنوان لایه پایه استفاده می‌کند، هر‌آنچه در شبکه آن اتفاق می‌افتد،‌ بر روی پراستفاده‌ترین و امن‌ترین بلاک‌چین حال حاضر، یعنی بیت‌کوین مستقر می‌شود. هدف شبکه استکس امکان اجرا و راه‌اندازی قراردادهای‌هوشمند و DAPPهای مختلف روی شبکه بیت کوین، بدون نیاز به فورک کردن یا تغییر بلاک چین اصلی بیت‌ کوین است.

**نحوه کارکرد شبکه استکس**

شبکه Stacks برای ایمن‌سازی بلاک‌چین خود از مکانیسم اثبات انتقال (Proof of Transfer) استفاده می‌کند. بر خلاف سایر پروژه‌های بلاک‌چین که از مکانیسم گواه اثبات کار (POW) و گواه اثبات سهام (POS) برای ایمن سازی شبکه خود استفاده می‌کنند، استکس الگوریتم اجماع جدیدی را توسعه داده است که برای انجام فعالیت‌های مختلف در شبکه و حفظ امنیت آن بسیار قوی عمل می‌کند. می‌توان گفت این مکانیسم به نوعی با توسعه مکانیسم اثبات سوزاندن (Proof of Burn) ایجاد شده است.

مکانیسم POB یک الگوریتم اجماع جایگزین است، که سعی می‌کند مشکل مصرف بالای انرژی در مکانیسم POW را حل کند. این مکانیسم به عنوان مکانیزم اثبات کار بدون اتلاف انرژی شناخته می‌شود و نحوه عملکرد آن مشابه مکانیسم اثبات سهام است؛ در هر دوی آن‌ها، ماینر‌ها با سپرده‌گذاری (Staking) کوین‌های خود، شبکه را ایمن کرده و در انجام تراکنش‌ها در شبکه ایفای نقش می‌کنند.

در مکانیسم POS ماینر‌ها به کوین‌های استیک کرده خود دسترسی دارند و می‌توانند آن‌ها را پس از مدتی برای فروش به بازار بیاورند؛ اما در مکانیسم گواه اثبات سوزاندن (POB)، کوین سپرده‌گذاری شده توسط ماینر‌ها سوزانده و از بین می‌رود و ماینرها دیگر به آن‌ها دسترسی ندارند.

اما مکانیسمی که شبکه استکس برای انجام عملیات بر بستر خود در نظر گرفته است، با نام مکانیسم اثبات انتقال (POX) شناخته می‌شود. تفاوت این روش با روش POB این است که سوزاندن کوین‌ها در آن انجام نمی‌پذیرد و به جای آن، ارز‌های دیجیتال استخراج شده در این شبکه، به سایر کاربران در این اکوسیستم منتقل می‌شوند. این مکانیزم به شبکه کمک می‌کند تا پروتکل پاداش‌دهی خود را تسهیل بخشد و به کاربران نیز اجازه می‌دهد همزمان در دو بلاک‌چین مختلف، فعالیت داشته باشند. همچنین از آن‌جایی که این شبکه با بلاک‌چین بیت‌کوین یک‌پارچه شده است، از یک بلاک چین بسیار امن برای ایمن کردن بلاک‌های جدید، بدون نیاز به مکانیسم POW بهره می‌برد. شبکه استکس از ۲ بخش ماینر‌ها و Stackها تشکیل می‌شود که در ادامه به توضیح آن‌ها می‌پردازم:

**ماینرها** **در شبکه Stacks**

با ساخت هر بلاک جدید در شبکه بیت‌ کوین، یک بلاک جدید در شبکه Stacks ساخته می‌شود. ماینرها در استکس به طور همزمان بلاک چین‌های هر دو شبکه را مشاهده می‌کنند. در شبکه استکس، ماینرها با ارسال BTC در شبکه بیت کوین، یک لیدر انتخاب می‌کنند؛ سپس یک تابع به‌صورت تصادفی لیدر هر دوره را با دادن وزن بیشتر به ماینر‌هایی که حجم بیشتری بیت کوین پرداخت کرده‌اند، انتخاب می‌کند. پس از انتخاب لیدر، بلاک جدید در بلاک چین استکس توسط او ساخته می‌شود. ماینر‌های این شبکه پس از انجام این کار پاداش خود را، هم از شبکه وهم از کارمزد تراکنش‌ها، بر اساس فرمول زیر دریافت می‌کنند.

* ۱۰۰۰ کوین STX به ازای هر بلاک در ۴ سال اول
* ۵۰۰ کوین STX به ازای هر بلاک در ۴ سال دوم
* ۲۵۰ کوین STX به ازای هر بلاک در ۴ سال سوم
* ۱۲۵ کوین STX به ازای هر بلاک بعد از اتمام دوره سوم؛ این ۱۲۵ کوین پاداش، برای همیشه در این شبکه ثابت خواهد بود.

هاوینگ‌ها (Halving) در این شبکه با هاوینگ در شبکه بیت کوین، به یک شکل انجام می‌پذیرد؛ همچنین ماینر‌ها برای ایجاد هر بلاک جدید، ۴۰ درصد از کارمزد شبکه را به صورت کوین STX دریافت می‌کنند و ۶۰ درصد باقی‌مانده نیز به ماینر‌هایی تعلق می‌گیرد که بلاک‌ها را تایید می‌کنند. دریافت این پاداش‌ها نیاز به ساخت ۱۰۰ بلاک در بلاک چین بیت کوین دارند و پس از ساخت این ۱۰۰ بلاک، ماینرها پاداش خود را پس از ۲۴ ساعت دریافت می‌کنند.

**هولدرها** **در شبکه Stacks**

هولدرها در این شبکه، در واقع استیک‌کنندگان توکن STX هستند؛ آن‌ها می توانند در اجماع این شبکه شرکت کنند و با استیکینگ یا سپرده‌گذاری کوین‌های STX خود به مدت تقریبا دو هفته، برای انجام سیکل تایید ۱۰۰۰۰ بلاک در شبکه بیت کوین، از شبکه استکس BTC پاداش بگیرند. همچنین Stackها می‌توانند به عنوان یک نود در شبکه استکس عمل کنند و اطلاعات تراکنش‌ها در این شبکه را در سیستم‌های خود ثبت کنند. بر خلاف مکانیسم POS که در آن اسلشینگ (Slashing) یا جریمه برای نودها در نظر گرفته می‌شود، در این شبکه این جریمه‌ها وجود ندارند.

**مقیاس پذیری تراکنش ها:**

تراکنش های بلاک چین Stacks می توانند مستقل از بیت کوین مقیاس شوند. آنها فقط برای تایید نهایی به بیت کوین وابسته هستند. هزاران تراکنش Stacks منجر به یک هش واحد در بیت کوین می شود. تراکنش‌های Stacks به‌عنوان بخشی از اجماع، هر بلوک بیت‌کوین را به‌طور خودکار روی بیت‌کوین توافق می‌کند. علاوه بر این، Stacks مفهوم میکروبلاک هایی را معرفی می کند که تایید اولیه را در چند ثانیه ارائه می دهند. میکروبلاک‌ها محل اصلی تحقیقات مقیاس‌پذیری آینده هستند، جایی که الگوریتم‌های اجماع سریع‌تر از نظر تئوری می‌توانند برای میکروبلاک‌هایی که داده‌ها را روی بیت‌کوین در هر بلوک بیت‌کوین توافق می‌کنند، اجرا شوند.

بیت کوین به عنوان یک پروتکل توافق توسط Stacks استفاده می شود. این به عنوان منبع حقیقت نهایی عمل می کند و هش های آرشیوی archives hashes تاریخچه بلوک Stacks را ذخیره می کند. نهایی بودن تراکنش ها در حال حاضر به بیت کوین **نود** خورده است و ما معتقدیم که بیت کوین مفهومی قوی از نهایی بودن ارائه می دهد که طراحی ما از آن سود می برد.

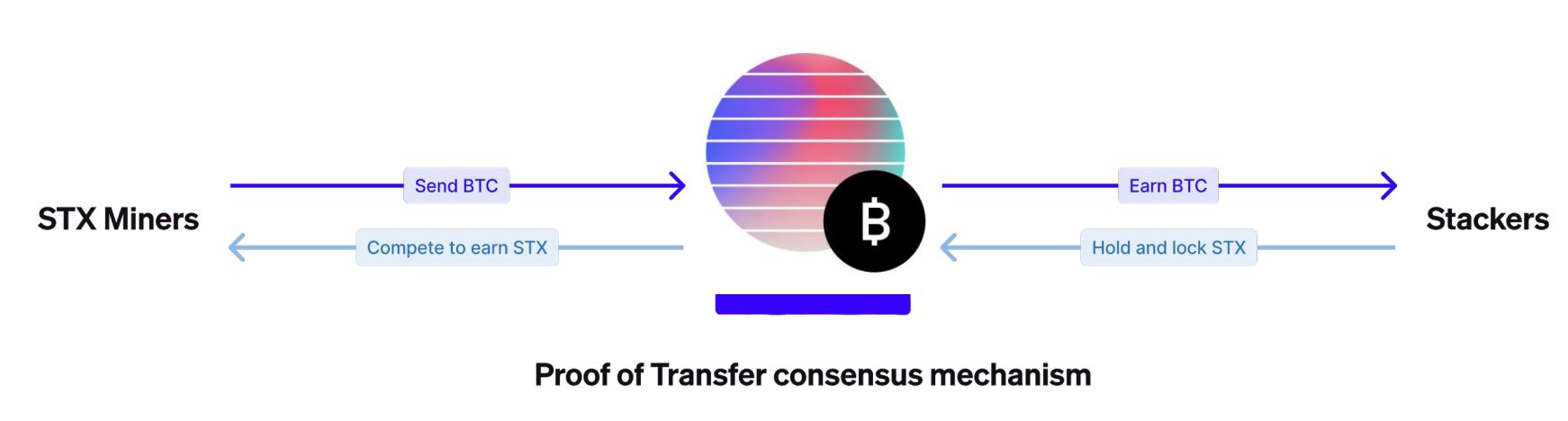
بلاک چین Stacks 2.0 به زبان Rust نوشته شده است. جزئیات پروتکل و open-source code در Stacks GitHub repository موجود است.

**الگوریتم اجماع PoX**

اثبات انتقال (PoX) اولین الگوریتم اجماع بین دو بلاک چین است. به طور خاص ما پیاده سازی PoX را با استفاده از بیت کوین به عنوان زنجیره پایه و Stacks به عنوان زنجیره متصل ارائه می کنیم. در PoX، انتخاب لیدر در بلاک چین بیت کوین اتفاق می افتد. به جای هدررفت انرژی بر روی اثبات کار، PoX از بیت کوین های قبلا ضرب شده به عنوان «اثبات محاسباتی» دوباره استفاده می کند و ماینرها هزینه استخراج بیت کوین خود را مستقیماً نشان می دهند.

ماینرهای STX برای تبدیل شدن به لیدر دور بعدی رقابت کردند. پروتکل ماینر برنده (یعنی لیدر) را با استفاده از یک تابع تصادفی قابل تأیید (VRF) انتخاب می کند. لیدر بلوک جدید بلاک چین Stacks را می نویسد و پاداش ها را می نویسد: stack های تازه ساخته شده برای بلوک، کارمزد قراردادهای هوشمند و تراکنش ها.

بیت‌کوین‌های مورد استفاده برای مناقصه‌های ماینر به مجموعه‌ای از آدرس‌های خاص مربوط به دارندگان توکن‌های Stacks (STX) ارسال می‌شوند که فعالانه در اجماع شرکت می‌کنند. بنابراین، بیت‌کوین‌های مصرف‌شده در فرآیند استخراج، به‌جای از بین رفتن، به‌عنوان پاداشی بر اساس داشتن Stacks و مشارکت در الگوریتم Stacking، به دارندگان Stacks مولد می‌رسند.



**قراردادهای هوشمند Clarity**

Clarity یک زبان برنامه نویسی جدید برای قراردادهای هوشمند است. زبان Clarity برای پیش بینی پذیری و امنیت بهینه می شود. Stacks 2.0 قراردادهای هوشمند را به بیت کوین متصل می کند و این امکان را برای قراردادهای هوشمند بر اساس اقدامات مشاهده شده در بلاک چین بیت کوین فراهم می کند.

قراردادهای هوشمند با طراحی خوب می توانند از باگ های احتمالی جلوگیری کنند، اما قراردادهای طراحی ضعیف می توانند مشکلات را تشدید کنند. این امر به ویژه با توجه به اینکه قراردادهای هوشمند برای نگه داشتن پول دیجیتال طراحی می شوند بسیار مهم است. با Clarity، رویکرد آنچه را که می‌بینید همان چیزی است که دریافت می‌کنید، اتخاذ کردیم. Clarity، هزینه و عملکرد قراردادهای هوشمند را هم برای توسعه دهندگان و هم برای تأیید خودکار شفاف می کند و شرایط پس از آن را برای ایمنی بیشتر معرفی می کند.

**زبان برنامه نویسی تصمیم پذیر:**

Clarity یک زبان قابل تصمیم است. یک زبان برنامه نویسی در صورتی قابل تصمیم گیری است که فرد بتواند با اطمینان از خودِ کد بداند که برنامه چه کاری انجام خواهد داد. Clarity عمداً تورینگ ناقص است زیرا از پیچیدگی تورینگ جلوگیری می کند. این امکان تجزیه و تحلیل استاتیک کامل کل نمودار تماس یک قرارداد هوشمند را فراهم می کند. علاوه بر این، پشتیبانی از انواع و نوع چک‌کننده می‌تواند کل کلاس‌های باگ مانند ارسال‌های ناخواسته، اشکال‌های ورود مجدد، و خواندن مقادیر اولیه را حذف کند. در نهایت، کد Clarity را می توان برای هزینه زمان اجرا و استفاده از داده تجزیه و تحلیل کرد. توسعه دهندگان می توانند پیش بینی کنند که یک برنامه Clarity چه کاری انجام می دهد و چقدر هزینه دارد.

Solidity، زبان پیاده‌سازی قراردادها در اتریوم زبانی غیرقابل تصمیم است: نمی‌توان دقیقاً دانست که یک قرارداد در موقعیت‌های خاص چگونه عمل می‌کند، بدون اینکه آن را واقعاً در آن موقعیت‌ها اجرا کنیم. هر دو نوع زبان برنامه نویسی مزایایی دارند. اما وقتی صحبت از قراردادهای هوشمند می شود که میلیاردها دلار کد را قفل می کنند، به حداقل رساندن خطرات بسیار مهم است.

**بدون کامپایلر:**

Clarity علاوه بر اینکه یک زبان قابل تصمیم است، تفسیر نیز می شود. کد منبع قرارداد خود توسط نود های بلاک چین منتشر و اجرا می شود. حذف هر گونه نمایش میانی و کامپایل شده (به عنوان مثال، کد بایت EVM برای Solidity) ، مساحت سطح را برای معرفی اشکالات به حداقل می رساند. انتشار کد منبع قرارداد نیز درک آن را بهبود می بخشد. باگ های کامپایلر در بلاکچین ها مضاعف آسیب می بینند، زیرا در حالی که کد منبع برنامه ریزی شده ممکن است خطا نداشته باشد، برنامه نهایی که به بلاک چین برسد می تواند. هر گونه چنین خطاهایی برای رفع نیاز به هارد فورک های بحث برانگیز - که به طور بالقوه غیرممکن هستند - دارند.

**قابل مشاهده در شبکه بیت کوین:**

قراردادهای Clarity در بیت کوین قابل مشاهده هستند، به این معنی که منطق قرارداد می تواند بر اساس تراکنش های بیت کوین فعال شود. قراردادهای Clarity دارای مدارک SPV داخلی برای بیت کوین هستند و می توانند تعامل با وضعیت بیت کوین را برای توسعه دهندگان بسیار آسان تر کنند. Clarity با بیت کوین فورک می شود، بنابراین توسعه دهندگان لازم نیست نگران موارد حاشیه ای باشند که در آن فورک ها و قراردادهای هوشمند بیت کوین باید با فورک تنظیم شوند.