سلام!

من علی طباطبایی هستم. مدتی رو در itorbit مشغول به کار بودم و این fork از bitcoin نتیجه ی بخشی از کاری بود که در شرکت انجام می دادم :)

لازمه این توضیح رو بدم که چون احتمال می دم نفر بعدی که این سورس کد رو بخونه، احتمالا ایرانی و عضوی از itorbit باشه، برای راحتی کار اون دارم فارسی می نویسم، و گرنه زبانم بد نیست :پی

خیلی نمی خوام طولانی کنم حرف رو، واسه همین به یه توضیح مختصر از کارای انجام شده می پردازم:

کلا ۱۲ تا commit از طرف من انجام شده:
-دو تا commit اول الکیه :))
- شش commit شماره ۳ تا ۸ یه سری پارامتر ها، از جمله خود genesis block، رو تو پروتکل bitcoin عوض کرده. نکته ی قابل ذکر اینه که در پایان این شش commit، کد همچنان به درستی کار نمی کند و این تغییرات در commit نهم است که به حالتی پایدار می رسیم.
- در commit نهم با تنظیم کردن difficulty و همچنین به دست آوردن genesis block ای که مطابق با آن difficulty است، اشکالات رفع شده و به اولین نسخه ای از کد تغییر یافته bitcoin می رسیم که به نظر به درستی کار می کند. در این مرحله تابعی نیز نوشته شد، که با صدا زدن آن، genesis block ای با block reward و difficulty ،timestamp دلخواه را می سازد.
- در commit دهم این بخش به کد اضافه می شود که تنظیمات genesis block را از روی فایل genesis.conf1 بخواند و که در خط اول و دوم timestamp و block reward است. اگر خط سوم در این فایل شامل عدد صفر بود، genesis block جدیدی تولید و اطلاعات دیگر شامل ،nonce merkleHash ،genesisHash را بر روی فایل genesis.conf2 بریزد. اگر خط سوم genesis.conf1 عدد ۱ بود، یعنی از اطلاعات genesis.conf2 نیز به عنوان ورودی استفاده می کند و genesis block قبلی را استفاده می کند.
- در commit یازدهم یک optimization کوچک برای تسریع در الگوریتم ساخت genesis block جدید انجام شده.
- در commit دوازدهم هم footprint رو به الگوریتم proof of work و در واقع به طور دقیقتر به تابع hash برای block ها اضافه کردم.

خب، آیا ۱۰۰٪ میشه گفت این تغییرات شامل هیچ باگی نیست؟ نمی تونم مطمین بگم، تا حد زیادی موقع coding دقت به عمل اومده ولی خب وقت واسه تست خیلی زیاد هم نبود، واسه همین نمیشه ۱۰۰٪ اطمینان داشت. البته خود bitcoin طوری پیاده سازی شده که اگه دست از پا خطا کنی ۱۰۰ جا با assertion و روش های دیگه بت گیر میده و در واقع وقتی به جایی برسی که گیر نمیده یعنی احتمال خطا پایینه واقعا.

سوال بعدی، آیا کاری که من کردم خیلی تغییر اساسی و کاملیه؟ خب نه واقعا، صرفا شروعی بوده واسه یه کار عظیم تر، یعنی امیدوارم اینجوری باشه.

خب، با این تفاسیر،این کارایی که من کردم، اصن به چه دردی می خوره؟ به نظرم مهم ترین نظرش اینه که کسی که commit های من رو به ترتیب بخونه، می تونه خیلی در فهمیدن سورس کد bitcoin جلو بیفته، چون روی کد هام خیلی دقیق comment گذاشتم و همچنین خود توضیح commit ها هم خیلی دقیقه. در واقع با خوندن توضیح commit ها و بعد از اون خوندن تغییراتی که تو commit داده شده و comment های مربوطه می تونین بفهمین که واسه ی تغییر یه سری چیز باید به کجای کد مراجعه کنید (این در حالت عادی کار زمان بری هست تو این سورس کد) و کلا ساختار سورس کد رو بیشتر درک می کنین. پیشنهادم اینه که وقتی مفاهیم نظری بیت کوین رو کامل فهمیدین و یکم سورس کد رو مطالعه کردین، این commit ها رو بررسی کنین که حدود چند روز ممکنه جلو بیفتین باهاش.

همین دیگه، مرسی