வெள்ளை அறிக்கை

பிட்காயின்

ஒரு பியர்-டு-பியர் மின்னணுசார் பண அமைப்பு

ஆசிரியர்

சட்டோசி நக்கமோட்டோ

தமிழாக்கம்

ராஜா சகாய ஜோஸ்

பிட்காயின்: ஒரு பியர்-டு-பியர் மின்னணுசார் பண அமைப்பு

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Translated in Tamil from bitcoin.org/bitcoin.pdf
By Raja Sahaya Jose @rajasahayajose

கருத்துச்சுருக்கம். ஒரு முழுமையான பியர்-டு-பியர் மின்னணுசார் பண அமைப்பானது, ஆன்லைன் பணத்தை, எந்தவொரு நிதி நிறுவனத்தின் குறுக்கீடுகளும் இல்லாமல், ஒரு தரப்பிலிருந்து மற்றொரு தரப்பிற்கு நேரடியாக அனுப்ப அனுமதிக்கிறது. டிஜிட்டல் கையொப்பங்கள் தீர்வின் ஒரு பகுதியை மட்டுமே நிறைவு செய்கிறது, ஆனால் இரட்டைச் செலவுகளை தடுக்க, மூன்றாம் தரப்பினரின் நம்பிக்கையானது இத்தீர்வுக்கு தேவைப்பட்டால், இந்தத் தீர்வு அளிக்கும் முக்கிய நன்மைகள் அனைத்தையும் இழக்கநேரிடும். பியர்-டு-பியர் வலையமைப்பைப் பயன்படுத்தி, இரட்டைச் செலவு சிக்கலுக்கு நாம் ஒரு புதிய தீர்வை முன்மொழிகிறோம். வலையமைப்புப் பரிமாற்றங்களின் காலமுத்திரைகளை ஹேஷ் ஆக மாற்றி, ஏற்கனவே தொடரும் ஹேஷ் அடிப்படையிலான, ப்ரூஃப்-ஆஃப்-வொர்க் சங்கிலித்தொடருக்குள் செலுத்துவதன் மூலம், ப்ரூஃப்-ஆஃப்-வொர்க் சங்கிலித்தொடரை மீண்டும் மறுஉருவாக்கம் செய்தால் மட்டுமே மாற்றம் செய்யக்கூடிய ஒரு பதிவு உருவாக்கப்படுகிறது. மிக நீளமான இந்தச் சங்கிலித்தொடரானது, நிகழ்வுகளின் வரிசைப்பதிவுக்கு மட்டும் சான்றாக இல்லாமல், கூடுதலாக கணினிகளின் மிகப் பெரிய கூட்டுத்திறனுக்கும் சான்றாக உள்ளது. இவ்வலையமைப்பை தாக்க ஒத்துழைக்காதக் கணினிமுனைகளால், பெரும்பாலான கணினித்திறன்கள் கட்டுப்படுத்தப்படும் வரை, மிக நீளமானச் சங்கிலித்தொடரை அவைகள் தொடர்ந்து உருவாக்குகிறது, மேலும் தாக்குதல்களையும் விஞ்சி நிற்கிறது. இத்தகைய வலையமைப்பிற்கு குறைந்தபட்ச கட்டமைப்பே தேவைப்படுகிறது. இவ்வலையமைப்பின் செய்திகள் சிறந்த முயற்சியின் அடிப்படையில் ஒளிபரப்பப்படுகின்றன, மேலும் கணினிமுனைகள் தங்கள் விருப்பப்படி வலையமைப்பிலிருந்து வெளியேறி மீண்டும் இணையலாம். வெளியேறியப் பிறகு நடந்த மாற்றங்களை மீண்டும் புதுப்பிக்க, மிக நீளமான ப்ரூஃப்-ஆஃப்-வொர்க் சங்கிலித்தொடரை சான்றாக ஏற்றுக்கொள்கிறது.

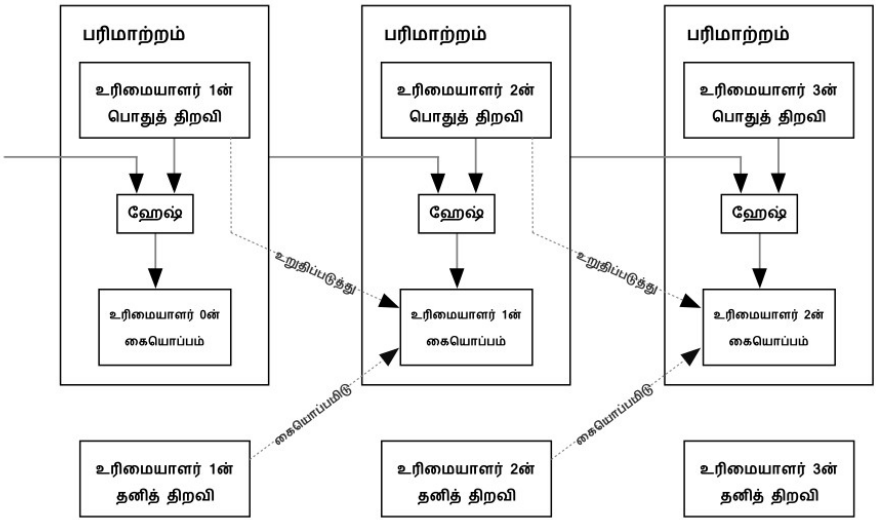
1. முகவுரை

இணைய வணிகமானது, மின்னணுசார் கட்டணங்களை நடைமுறைப்படுத்த, நம்பகமான மூன்றாம் தரப்பினராக பெரும்பாலும் நிதி நிறுவனங்களையே சார்ந்திருக்கிறது. இந்த அமைப்புகள், பெரும்பாலான பரிமாற்றங்களுக்கு போதுமானத் தேவையை நிறைவு செய்தாலும், நம்பிக்கை அடிப்படையிலான மாதிரியில் உள்ள, உள்ளார்ந்த பலவீனங்களால் வெகுவாகப் பாதிக்கப்படுகிறது. நிதி நிறுவனங்களால் கருத்துவேறுபாடுகளுக்கானத் தலையீட்டை தவிர்க்க முடியாது என்பதால், முற்றிலும் மீளாப் பரிமாற்றங்கள் ஒருபோதும் சாத்தியப்படாது. தலையீடுகளுக்கானச் செலவுகளால் பரிமாற்றங்களின் செலவுகள் அதிகரிக்கிறது, நடைமுறை பரிமாற்றங்களின் குறைந்தபட்ச அளவுகள் கட்டுப்படுத்தப்படுகிறது, மேலும் சிறிய சாதாரண பரிமாற்றங்களின் சாத்தியக்கூறுகள் துண்டிக்கப்படுகிறது, மற்றும் மீளாச் சேவைகளுக்காக செலுத்தப்படும் மீளாக் கட்டணங்களை நடைமுறைப்படுத்தும் திறமின்மையால், அதற்கானச் செலவானது பரவலாக வசூலிக்கப்படுகிறது. மீளும் சாத்தியக்கூறுகளுடன், நம்பிக்கைக்கானத் தேவையானது பரவலாக்கப்படுகிறது. வணிகர்கள் கட்டாயம் தங்கள் வாடிக்கையாளர்களிடம் முன்னெச்சரிக்கையாக இருக்கவேண்டும் என்பதால், தேவைக்கு அதிகமான தகவல் வேண்டி அவர்கள் இடையூரு செய்யப்படுகிறார்கள். ஒரு குறிப்பிட்ட சதவிகித மோசடியானது தவிர்க்க முடியாத ஒன்றாக ஏற்றுக்கொள்ளப்படுகிறது. இயல் நாணயத்தை நேரடியாகப் பயன்படுத்துவதன் மூலம், செலவுகள் மற்றும் கட்டணங்களின் நிச்சயமற்றத் தன்மைகளை தவிர்க்கலாம், ஆனால் தொடர்புச் செல்வழி மூலம், நம்பகமானத் தரப்பினர் இல்லாமல் பணம் செலுத்தும் இயக்கமுறைகள் இதுவரை இல்லை.

என்ன தேவையென்றால், நம்பிக்கைக்கு மாற்றாக, மறைக்குறியீட்டின் ஆதார அடிப்படையில் இயங்கும் ஒரு மின்னணுசார் பண அமைப்பு, மற்றும் நம்பகமான மூன்றாம் தரப்பின் தேவையே இல்லாமல், விருப்பமுள்ள எந்த இரண்டுத் தரப்பினரும் நேரடியாகத் தங்களுக்குள் பணப் பரிமாற்றம் செய்வதற்கான அனுமதி. கணக்கீடுகளால் மீள் செய்ய சாத்தியமற்றப் பரிமாற்றங்களானது, மோசடிகளிலிருந்து விற்பனையாளர்களைப் பாதுகாக்கும், மேலும் வழக்கமான எஸ்க்ரோ இயக்கமுறைகளை எளிமையாகச் செயல்படுத்தி வாங்குபவர்களையும் பாதுகாக்கலாம். இந்த அறிக்கையில், இரட்டைச் செலவு சிக்கலுக்கு நாம் முன்மொழியும் தீர்வானது, பியர்-டு-பியர் அமைப்பின், பரவலாக்கப்பட்ட காலமுத்திரைச் சேவையகத்தை பயன்படுத்தி, பரிமாற்றங்களுடையக் காலவரிசையின் கணக்கீட்டு ஆதாரத்தை உருவாக்குகிறோம். நேர்மையானக் கணினிமுனைகளின், கூட்டுப் பெரும்பான்மையால் கட்டுப்படுத்தப்படும் கணினித் திறனானது, ஒன்றுபட்டக் குழுவாகத் தாக்கும் கணினிமுனைகளின் திறனைவிட அதிகமாக இருக்கும் வரை, இந்த அமைப்பு பாதுகாக்கப்படுகிறது.

2. பரிமாற்றங்கள்

நாம் மின்னணுசார் நாணயத்தை, டிஜிட்டல் கையொப்பங்களின் சங்கிலித்தொடராக வரையறுக்கிறோம். உரிமையாளர்கள் ஒவ்வொருவரும் நாணயத்தை அடுத்தவருக்கு அனுப்ப, டிஜிட்டல் கையொப்பமிட்ட முந்தைய பரிமாற்றத்தின் ஹேஷ் மற்றும் அடுத்த உரிமையாளரின் பொதுத் திறவி ஆகியவைகளை நாணயத்தின் முடிவில் சேர்க்கின்றனர். பணம் பெறும் ஒருவரால், கையொப்பங்களை உறுதிசெய்வதன் மூலம், சங்கிலித்தொடரின் உரிமையை உறுதிசெய்ய முடியும்.

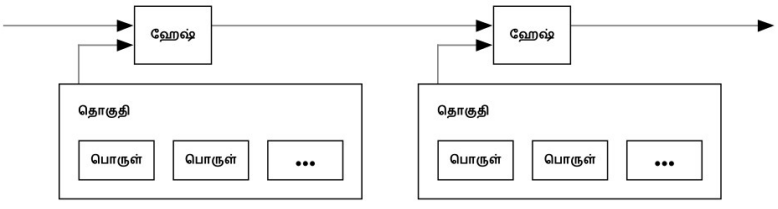


இங்கு உண்மையான சிக்கல் என்னவென்றால், உரிமையாளர்களில் ஒருவரின் நாணயமாவது இரட்டைச் செலவுக்கு உள்ளாகவில்லை என்பதை, பணம் பெறுபவரால் ஒருபோதும் உறுதிசெய்ய முடியாது. நம்பகமான மத்திய அதிகாரம் அல்லது மின்ட்டை ஒரு பொதுவானத் தீர்வாக அறிமுகப்படுத்துவதன் மூலம், ஒவ்வொரு பரிமாற்றத்திலும் இரட்டைச் செலவுகளானது சரிபார்க்கப்படுகிறது. ஒவ்வொரு பரிமாற்றத்திற்குப் பிறகு அந்த நாணயமானது, மின்ட்டிற்க்கு கட்டாயமாகத் திருப்பி அனுப்பப்பட்டு, புதிய நாணயம் வெளியிடப்படுகிறது. மற்றும் மின்ட்டால் வெளியிடப்பட்ட நாணயங்களானது இரட்டைச் செலவுக்கு உள்ளாகாத ஒன்றாக நம்பப்படுகிறது. இந்தத் தீர்வின் சிக்கல் என்னவென்றால், இந்த பண அமைப்பின் முழுத் தலைவிதியும், மின்ட்டை நடத்தும் நிறுவனத்தைப் பொறுத்தே நிர்ணயிக்கப்படுகிறது. மேலும் வங்கியைப் போலவே ஒவ்வொரு பரிமாற்றங்களும் இதன் மூலம் சென்றாக வேண்டும்.

முந்தைய உரிமையாளர்கள், எந்த முன் பரிமாற்றத்திற்கும் கையொப்பமிடவில்லை என்பதை, பணம் பெறுபவர் தெரிந்துகொள்ள நமக்கு ஒரு வழி தேவைப்படுகிறது. நம்முடைய தேவைகளுக்காக ஆரம்ப பரிமாற்றம் ஒன்றே கணக்கில் எடுத்துக்கொள்ளப்படுகிறது, ஆதலால் பின்னர் நடக்கும் இரட்டைச் செலவுக்கான முயற்சிகள் பற்றி நாம் கவலைப்பட தேவையில்லை. அனைத்துப் பரிமாற்றங்கள் பற்றி அறிந்திருப்பதே, இல்லாதப் பரிமாற்றத்தை உறுதிப்படுத்த ஒரே வழி. மின்ட் அடிப்படையிலான மாதிரியில், மின்ட்டானது அனைத்துப் பரிமாற்றங்களையும் அறிந்திருக்கும், மேலும் முதலில் எது வந்தது என்பதையும் முடிவு செய்யும். நம்பகமானத் தரப்பினர் இல்லாமல் இதைச் செய்துமுடிக்க, பரிமாற்றங்கள் அனைத்தும் கட்டாயம் பொதுப்படையாக அறிவிக்கப்படவேண்டும் [1], மேலும் பங்கேற்பாளர்கள், ஒரு ஒற்றை நிகழ்ச்சிக்கோவையை அவைப் பெறப்பட்ட வரிசைபடியே ஒப்புக்கொள்ள, நமக்கு ஒரு அமைப்பு தேவை. ஒவ்வொரு பரிமாற்ற நேரத்தின் போதும், இதை முதலில் பெற்றதாக பெரும்பான்மையானக் கணினிமுனைகள் ஒப்புக்கொள்வதே, பணம் பெறுபவருக்குத் தேவைப்படும் ஆதாரமாகும்.

3. காலமுத்திரைச் சேவையகம்

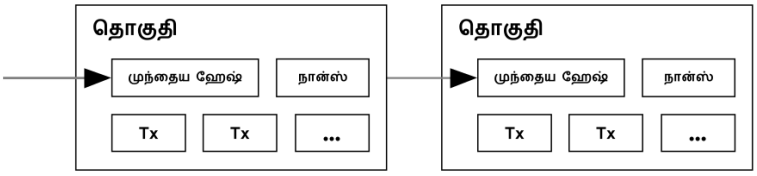
நாம் முன்மொழியும் தீர்வானது காலமுத்திரைச் சேவையகத்துடன் தொடங்குகிறது. ஒரு காலமுத்திரைச் சேவையகத்தின் வேலையானது, காலமுத்திரையிடப்பட வேண்டிய தொகுதிப் பொருட்களின் ஹேஷ்யை ஏற்றுக்கொள்ளுவதும், மற்றும் செய்தித்தாள் அல்லது யூஸ்நெட் இடுகையைப் [2-5] போல அந்த ஹேஷ்யை பரவலாக வெளியிடுவதும். உண்மையில் ஹேஷ்யில் நுழைவதற்காகவே, இந்தப் பதிவானது இந்த நேரத்தில் இருந்திருக்க வேண்டும் என்பதை காலமுத்திரை நிருபிக்கிறது. ஒவ்வொரு காலமுத்திரையும் அதற்கு முந்தைய காலமுத்திரையின் ஹேஷ்யை உள்ளடக்கி, சங்கிலித்தொடர் ஒன்றை உருவாக்குகிறது, ஒவ்வொரு கூடுதலானக் காலமுத்திரையுடன் அதற்க்கு முன்னால் உள்ளவைகளை வலுப்படுத்துகிறது.



4. ப்ரூஃவ்-ஆஃப்-வொர்க்

பரவலாக்கப்பட்ட காலமுத்திரைச் சேவையகத்தை, பியர்-டு-பியர் அடிப்படையில் செயல்படுத்த நமக்குத் தேவைப்படுவது, செய்தித்தாள் அல்லது யூஸ்நெட் இடுகைகள் போல் அல்லாத, ஆனால் ஆடெம் பேக்கினுடைய ஹேஷ்கேஷ் [6] போல் உள்ள ஒரு ப்ரூஃவ்-ஆஃப்-வொர்க் அமைப்பு. SHA-256 போன்றவைகளால் ஹேஷ் செய்யும்போது, உருவாகும் மதிப்பை ஸ்கேனிங் செய்யவே ப்ரூஃவ்-ஆஃப்-வொர்க்கானது ஈடுபடுத்தப்படுகிறது, இந்த ஹேஷ்யானது பல பூஜ்ஜியப் பிட்கள் உடன் தொடங்குகிறது. பூஜ்ஜியப் பிட்கள் எண்ணிக்கையின் தேவையைப் பொறுத்து, அதற்குத் தேவைப்படும் சராசரி வேலையின் அடுக்கேற்றமானது அமையும், மேலும் ஒற்றை ஹேஷ்யை இயக்குவதன் மூலம், இதனை உறுதிசெய்து கொள்ள முடியும்.

நம்முடைய காலமுத்திரை வலையமைப்புக்கு, ப்ரூஃவ்-ஆஃப்-வொர்க்கை நாம் செயல்படுத்தி, தொகுதியின் ஹேஷ்க்குத் தேவையான பூஜ்ஜியப் பிட்களை வழங்கும் மதிப்பானது கண்டறியப்படும் வரை, தொகுதியில் உள்ள நான்ஸ்யை அதிகரிக்கிறோம். ஒருமுறை கணினியின் முயற்சியைச் செலவிட்டு ப்ரூஃவ்-ஆஃப்-வொர்க்கை நிறைவுசெய்தப் பிறகு, அதே வேலையை மீண்டும் செய்யாமல் அந்தத் தொகுதியை மாற்ற முடியாது. பிந்தையத் தொகுதிகள் எல்லாம் சங்கிலியாக அதற்குபின் இணைக்கப்பட்டுள்ளதால், அந்தத் தொகுதியை மாற்றுவதற்கான வேலை என்பது, பின்னால் உள்ளத் தொகுதிகளை எல்லாம் மீள்உருவாக்கம் செய்வதையும் உள்ளடக்கியது.



பெரும்பான்மைத் தீர்மானத்தை எடுப்பதற்கான, பிரதிநிதித்துவத்தை நிர்ணயிக்கும் சிக்கலுக்கும் ப்ரூஃவ்-ஆஃப்-வொர்க்கானது தீர்வு அளிக்கிறது. ஒரு-ஐபி-முகவரி-ஒரு-ஓட்டு அடிப்படையில் பெரும்பான்மையானவர்கள் இருந்தால், பல ஐபிகளை உருவாக்க முடிந்த யாராலும் அது வீழ்த்தப்படலாம். ப்ரூஃவ்-ஆஃப்-வொர்க்கானது ஒரு-கணினி-ஒரு-ஓட்டு அடிப்படையிலான ஒன்று. பெரும்பான்மை முடிவானது மிக நீளமானச் சங்கிலித்தொடரால் தீர்மானிக்கப்படுகிறது, அதில் ப்ரூஃவ்-ஆஃப்-வொர்க்குக்காக முதலீடுச் செய்யப்பட்ட ஆற்றலானது மிகப்பெரிதாக உள்ளது. பெரும்பான்மையானக் கணினித் திறனானது நேர்மையானக் கணினிமுனைகளால் கட்டுப்படுத்தப்படும் வரை, நேர்மையானச் சங்கிலித்தொடரே அதிவேகமாக வளரும் மற்றும் போட்டியில் பங்குகொள்ளும் மற்றச் சங்கிலித்தொடர்களையும் விஞ்சி நிற்கும். கடந்தத் தொகுதியில் மாற்றம் செய்ய, தாக்குபவர் ஒருவர் செய்யவேண்டியது, அந்தத் தொகுதி மற்றும் அதற்கு பின்னால் உள்ள அனைத்துத் தொகுதிகளையும் ப்ரூஃவ்-ஆஃப்-வொர்க்கைப் பயன்படுத்தி மீள்உருவாக்கம் செய்யவேண்டும், மேலும் நேர்மையானக் கணினிமுனைகளுக்கு ஈடுகொடுத்து அதை விஞ்ச வேண்டும். மெதுவாகத் தாக்குபவர் ஈடுகொடுப்பதற்கான நிகழ்தகவானது, அடுத்து வரும் தொகுதிகளின் இணைப்பிற்கு ஏற்ப, அடுக்கேற்றமுறையில் அதிவேகமாகக் குறைகிறது என்பதை நாம் பின்னர் காண்பிப்போம்.

அதிகரிக்கும் வன்பொருளின் வேகத்திற்கும், மற்றும் காலப்போக்கில் கணினிமுனைகளை இயக்குவதில் உள்ள மாறுபட்ட ஆர்வத்தையும் ஈடுசெய்வதற்காக, ஒரு மணி நேரத்தில் உருவாக்கப்படும் தொகுதியின் சராசரி எண்ணிக்கையை, இலக்காகக் கொண்டு நகரும் சராசரியால் ப்ரூஃவ்-ஆஃப்-வொர்க்கின் கடினமானது தீர்மானிக்கப்படுகிறது. மிக வேகமாக அவைகள் உருவாக்கப்பட்டால் அதன் கடினமும் அதிகரிக்கிறது.

5. வலையமைப்பு

வலையமைப்பை இயக்குவதற்கானப் படிகள் பின்வருமாறு:

1) புதியப் பரிமாற்றங்களானது அனைத்துக் கணினிமுனைகளிலும் ஒளிபரப்பப்படுகிறது.
2) ஒவ்வொரு கணினிமுனையும் புதியப் பரிமாற்றங்களை ஒரு தொகுதிக்குள் சேகரிக்கிறது.
3) ஒவ்வொரு கணினிமுனையும் அதன் தொகுதிக்கான கடினமானப் ப்ரூஃவ்-ஆஃப்-வொர்க்கை கண்டறிவதற்கான வேலையைச் செய்கிறது.
4) ஒரு கணினிமுனையானது ப்ரூஃவ்-ஆஃப்-வொர்க்கை கண்டறியும் போது, அந்தத் தொகுதியை எல்லாக் கணினிமுனைகளுக்கும் ஒளிபரப்புகிறது.
5) சரியான மற்றும் ஏற்கனவேச் செலவழியாத பரிமாற்றங்களின் தொகுதியை மட்டுமே கணினிமுனைகள் ஏற்றுக்கொள்கிறது.
6) கணினிமுனைகளானது சங்கிலித்தொடரில் உள்ள அடுத்தத் தொகுதியை உருவாக்குவதன் மூலம் தொகுதியை ஏற்பதை வெளிப்படுத்துகிறது, ஏற்கப்பட்டத் தொகுதியின் ஹேஷ்யை, முந்தைய ஹேஷ்யாக பயன்படுத்துகிறது.

கணினிமுனைகள் எப்போதும் நீளமானச் சங்கிலித்தொடரையே சரியான ஒன்றாக கருதுகின்றன, மேலும் அவைகள் அதை நீட்டிக்க தொடர்ந்து அதன் வேலையை செய்து கொண்டிருக்கும். இரண்டு கணினிமுனைகள் அடுத்தத் தொகுதியின் வெவ்வேறு பதிப்புகளை ஒரே நேரத்தில் ஒளிபரப்பினால், சில கணினிமுனைகள் ஒன்று அல்லது மற்றொன்றை முதலில் பெறலாம். இந்த சூழலில், அவர்கள் முதலில் பெறப்பட்டதையே செயல்படுத்துகிறார்கள், ஆனால் மற்றக் கிளையானது நீளும் சாத்தியத்தைப் பொறுத்து

அதையும் சேகரிக்கிறார்கள். அடுத்தப் ப்ரூஃப்-ஆஃப்-வொர்க் கண்டறியப்பட்டு ஒரு கிளை நீளமாகும் போது சமநிலையானது உடைக்கப்படுகிறது, மற்றக் கிளையில் செயல்படும் கணினிமுனைகளானது நீண்டக் கிளைக்கு மாறுகிறது.

புதியப் பரிமாற்றத்தின் ஒளிபரப்பானது எல்லாக் கணினிமுனைகளையும் அடைய வேண்டிய அவசியமில்லை. ஆனால் பலக் கணினிமுனைகளை அவைகள் அடைந்தவுடனேயே, எவ்விதத் தாமதமின்றி ஒரு தொகுதியைச் சென்று அடைந்திருக்கும். தொகுதியின் ஒளிபரப்புகள் கைவிடப்பட்டச் செய்திகளையும் பொறுத்துக்கொள்கிறது. ஒரு கணினிமுனையானது தொகுதி ஒன்றைப் பெறவில்லை என்றால், அது அடுத்தத் தொகுதியை பெறும்போது, தவறவிட்ட ஒன்றை உணர்ந்து அதற்கான கோரிக்கையை வைக்கிறது.

6. ஊக்கத்தொகை

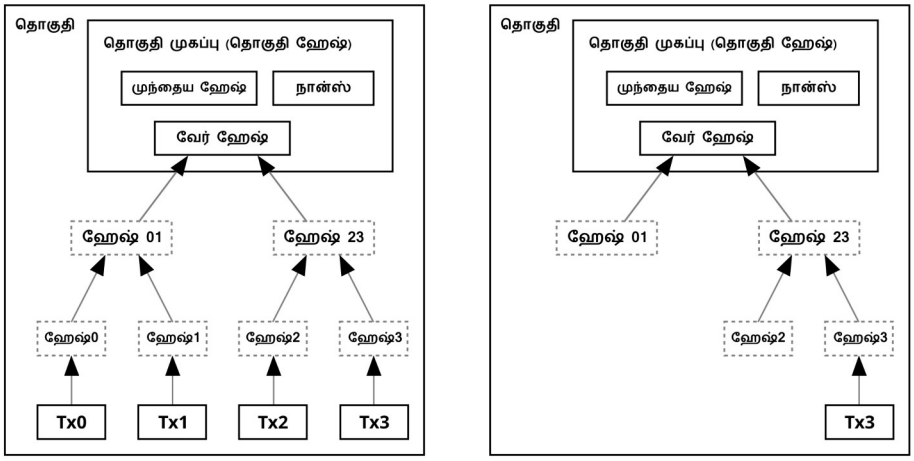
மரபுப்படி, ஒரு தொகுதியின் முதல் பரிமாற்றம் என்பது, அந்தத் தொகுதியை உருவாக்கியவருக்கு சொந்தமான, ஒரு புதிய நாணயத்தைக் கொண்டு ஆரம்பிக்கும் ஒரு சிறப்பு பரிமாற்றம் ஆகும். கணினிமுனைகளுக்கான ஊக்கத்தொகையைச் சேர்ப்பதன் மூலம் அந்த வலையமைப்புக்கான ஆதரவானது அளிக்கப்படுகிறது, மேலும் நாணயங்களை வெளியிடும் மத்திய அதிகாரம் இல்லாத பட்சத்தில், ஆரம்பத்திலேயே அவைகளை விநியோகிக்கும் ஒரு வழிமுறையையும் இதன்முலம் வழங்குகிறது. நிலையாகச் சேர்க்கப்படும் மாறா அளவுடைய புதிய நாணயங்களானது, தங்கச்சுரங்கத் தொழிலாளர்கள் தங்கள் வளங்களை செலவிட்டு தங்கத்தை புழக்கத்தில் சேர்ப்பதற்கு ஒப்பாகும். நம்முடைய விடயத்தில் கணினியின் நேரம் மற்றும் மின்சாரம் செலவழிக்கப்படுகிறது.

பரிமாற்றக் கட்டணத்தை பயன்படுத்தியும் ஊக்கத்தொகையின் நிதியானது வழங்கப்படலாம். ஒரு பரிமாற்றத்தின் வெளியீட்டு மதிப்பு அதன் உள்ளீட்டு மதிப்பை விட குறைவானால், அந்த வேறுபாடானது பரிமாற்றக் கட்டணமாக மாற்றப்பட்டு, அந்த பரிமாற்றத்தை உள்ளடக்கியத் தொகுதியின் ஊக்க மதிப்பில் சேர்க்கப்படுகிறது. முன்னரே தீர்மானிக்கப்பட்ட எண்ணிக்கையிலுள்ள நாணயங்கள் ஒருமுறை புழக்கத்தில் நுழைந்தவுடன், ஊக்கத்தொகையானது முற்றிலுமாக பரிமாற்றக் கட்டணமாக மாற்றப்பட்டு, பணவீக்கத்திலிருந்தும் முழு விடுதலையளிக்கிறது.

ஊக்கத்தொகையானது கணினிமுனைகளை ஊக்குவித்து நேர்மையாக இருக்க உதவிசெய்யும். பேராசையால் தாக்கும் ஒருவரால், அனைத்து நேர்மையானக் கணினிமுனைகளை விட அதிகமான கணினித் திறனை ஒன்று சேர்க்க முடிந்தால், அதைப் பயன்படுத்தி இவற்றிற்கிடையில் அவரால் தேர்வு செய்ய முடிவது மக்களை ஏமாற்றி அவர் பணத்தைத் திரும்பப் பெறுவது அல்லது புதிய நாணயங்களை உருவாக்குவது. மாறாக அவர் வேண்டிய விதிமுறைகளைக் கடைபிடிக்கும் போது அதிக லாபம் பெறுவதை கண்டறிகிறார், அத்தகைய விதிமுறைகள் அவருக்குச் சாதகமாக இருந்து, மற்ற அனைவரும் இணைந்து பெறுவதைவிட அதிகமான புதிய நாணயங்களை அவருக்குப் பெற்றுத்தருகிறது, மேலும் அமைப்பைக் குறைமதிப்பிற்கு உட்படுத்துவதால் மற்றும் சொந்தச் செல்வத்தின் பெறுமானத்தால் கிடைப்பதை விட அதிகமாக பெறுகிறார்.

7. வட்டு இடவெளி மீட்டெடுப்பு

ஒரு நாணயத்தின் சமீபத்தியப் பரிமாற்றமானது போதுமானத் தொகுதிகளின் கீழ் புதைக்கப்பட்டவுடன், அதற்கு முந்தைய செலவழிக்கப்பட்டப் பரிமாற்றத்தை நீக்குவதன் மூலம் வட்டு இடவெளியை சேமிக்கலாம். தொகுதியினுடைய ஹேஷ்யை சேதப்படுத்தாமல் இதை எளிதாக்குவதற்கு, பரிமாற்றங்களானது ஒரு மெர்க்கல் மரத்தில் [7][2][5] ஹேஷ் செய்யப்படுகின்றன. தொகுதியினுடைய ஹேஷ்யுடன் வேர் மட்டுமே சேர்க்கப்படுகிறது. மரத்தின் கிளைகளைத் துண்டிப்பதன் மூலம் பழையத் தொகுதிகளை சுருக்கமுடியும். மேலும் உட்புறமுள்ள ஹேஷ்களை சேமிக்க தேவையில்லை.



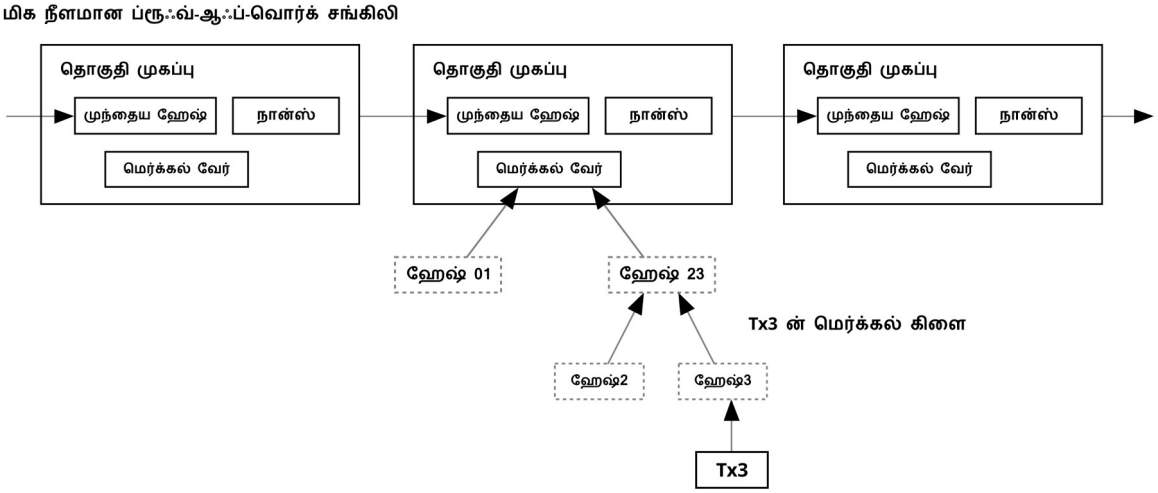
ஒரு மெர்க்கல் மரத்தில் பரிமாற்றங்கள் ஹேஷ்யாகிறது

தொகுதியிலிருந்து **Tx0-2** நீக்கியப்பிறகு

பரிமாற்றங்கள் இல்லாத தொகுதியின் முகப்பானது சுமார் 80 பைட்டுகளாக இருக்கும். ஒவ்வொரு 10 நிமிடங்களுக்கும், தொகுதிகளானது உருவாக்கப்படுவதாக வைத்துக் கொண்டால், 80 பைட்டுகள் * 6 * 24 * 365 = 4.2MBஆண்டுக்கு. 2008 இல், கணினி அமைப்புகளுடன் பொதுவாக விற்பனை செய்யப்படும் தற்காலிக நினைவகம் 2GB, மற்றும் மூரின் சட்டம் முன்னறிவிக்கும் தற்போதைய வளர்ச்சியானது ஆண்டுக்கு 1.2GB, எனவே தொகுதியின் முகப்புகளை தற்காலிக நினைவகத்தில் வைத்திருந்தாலும் சேமிப்பகம் ஒருச் சிக்கலாக இருக்காது.

8. எளிமையாக்கப்பட்ட கட்டணச் சரிபார்ப்பு

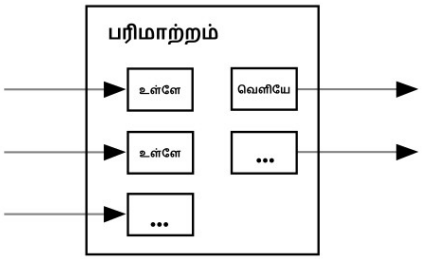
ஒரு முழு வலைக் கணினிமுனையை இயக்காமலே, பணம் செலுத்துவதைச் சரிபார்க்க முடியும். நீண்ட ப்ரூஃவ்-ஆஃப்-வொர்க் சங்கிலித்தொடரின் தொகுதி முகப்புகளின் நகல் ஒன்றே ஒரு பயனருக்குத் தேவையானது, தன்னிடம் மிக நீளமானச் சங்கிலித்தொடர் இருப்பதாக அவருக்கு நம்பிக்கை வரும்வரை, வலைக் கணினிமுனையை வினவி அதை அவர் பெறலாம், மற்றும் காலமுத்திரையிடப்பட்டப் பரிமாற்றத்தை கொண்டத் தொகுதியுடன் இணைந்திருக்கும் மெர்க்கல் கிளையையும் பெறலாம். பரிமாற்றங்களைச் சரிபார்க்க அவரால் முடியாது, ஆனால் சங்கிலித்தொடரில் உள்ள ஒரு இடத்தில் அதை இணைப்பதன் மூலம், ஒரு வலைக் கணினிமுனை அதனை ஏற்றுக்கொண்டதை அவரால் பார்க்க முடியும், மேலும் பின்னால் சேர்க்கப்பட்டத் தொகுதிகளானது அந்த வலையமைப்பு ஏற்றுக்கொண்டதை மேலும் உறுதிப்படுத்துகிறது.



ஆகவே, நேர்மையானக் கணினிமுனைகளால் வலையமைப்புக் கட்டுப்படுத்தப்படும் வரை சரிபார்ப்பு நம்பகமானதாக இருக்கும், ஆனால் தாக்குபவர் ஒருவரின் அதிகாரமானது வலையமைப்பில் அதிகரிக்கும் போது அது பாதிப்புக்குள்ளாகலாம். தங்களுக்கானப் பரிமாற்றங்களை வலைக் கணினிமுனைகளால் சரிபார்க்க முடியும் வேளையில், தாக்குபவரின் விஞ்சிய அதிகாரமானது வலையமைப்பில் தொடரும்வரை, எளிமைப்படுத்தப்பட்ட முறையை, தாக்குபவரால் புனையப்பட்ட பரிமாற்றங்களால் ஏமாற்றமுடியும். இதற்கு எதிரான ஒரு பாதுகாப்பு யுக்தியாக, வலைக் கணினிமுனைகள் தவறானத் தொகுதியை கண்டறியும் போது, அவைகளிலிருந்து வரும் விழிப்பூட்டல்களை ஏற்கவேண்டும், முழுத் தொகுதியையும் பதிவிறக்கம் செய்ய பயனரின் மென்பொருளைத் தூண்டவேண்டும், மற்றும் முரண்பாட்டை உறுதிப்படுத்த பரிமாற்றங்களை எச்சரிக்கவேண்டும். அடிக்கடி பணம் பெறும் வணிகங்கள், இன்னும் அதிகச் சுதந்திரமான பாதுகாப்பு மற்றும் விரைவானச் சரிபார்ப்புக்காக தங்கள் சொந்த முனைகளை இயக்க விரும்பலாம்.

9. மதிப்பை இணைத்தல் மற்றும் பிரித்தல்

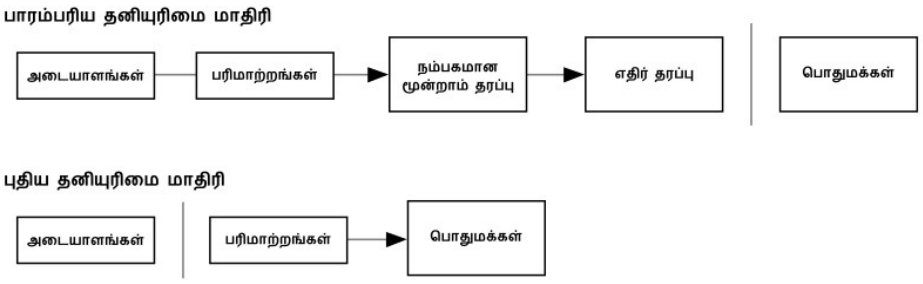
நாணயங்களை தனித்தனியாகக் கையாள முடியும் என்றாலும், ஒவ்வொரு சென்ட்டின் பரிமாற்றத்திற்கும் தனித்தனிப் பரிமாற்றத்தை உருவாக்குவது பயனற்றதாக இருக்கும். பரிமாற்றங்களில் உள்ள பல உள்ளீடுகள் மற்றும் வெளியீடுகள் மதிப்பைப் பிரித்து இணைக்க அனுமதிக்கிறது. பொதுவாக, முந்தைய பெரியப் பரிமாற்றத்திற்கு ஒரு உள்ளீடு இருக்கும் அல்லது சிறிய தொகைகளை இணைக்கும் பல உள்ளீடுகள் இருக்கும், மேலும் அதிகபட்சமாக இரண்டு வெளியீடுகள்: பணம் செலுத்துவதற்கு ஒன்று மற்றும் ஏதேனும் மீதம் இருந்தால் அனுப்புநரிடம் சில்லறையைத் திருப்பியனுப்ப ஒன்று.



ஒரு பரிமாற்றமானது, பல பரிமாற்றங்களைச் சார்ந்திருக்கும் போது, அது வெளிப்புறமாக விரிகிறது என்பதை கவனத்தில் கொள்ள வேண்டும், மேலும் அதிகமானப் பரிமாற்றங்களை சார்ந்து இருக்கும் பரிமாற்றங்கள் இங்கு ஒரு சிக்கல் இல்லை. முழுமையாகத் தனித்தியங்கும் ஒரு பரிமாற்றத்தின் நிகழ்ச்சிக்கோவை நகலை, இங்கு பிரித்தெடுக்க வேண்டிய அவசியமே இல்லை.

10. தனியுரிமை

பாரம்பரிய வங்கியின் மாதிரியானது, சம்பந்தப்பட்டத் தரப்பினர்களின் மற்றும் நம்பகமான மூன்றாம் தரப்பின், தகவலுக்கான அணுகலைக் கட்டுப்படுத்துவதன் மூலம், தனியுரிமை நிலையை அடைகிறது. அனைத்துப் பரிமாற்றங்களையும் வெளிப்படையாக அறிவிக்க வேண்டிய அவசியத்தை இந்த முறையானது தடுக்கிறது, ஆனால் இதன் தகவல் ஓட்டத்தை மற்றொரு இடத்தில் தகர்ப்பதன் மூலம், அதாவது பொதுத் திறவிகளை மறைத்து வைப்பதால், தனியுரிமையை இன்னும் பராமரிக்க முடியும். பரிமாற்றத்தை யாருடனும் இணைக்கும் தகவல்கள் இல்லாமல், யாரோ ஒருவர் ஒரு தொகையை வேறொருவருக்கு அனுப்புவதை பொதுமக்களால் பார்க்கமுடியும். இது பங்குச் சந்தைகள் தனிப்பட்ட வணிகத்தின் நேரம் மற்றும் அளவு சார்ந்து வெளியிடும் தகவல்களைப் போன்றது, ஆனால் யார் தரப்பினர்கள் என்று சொல்லாமல் "டேப்" பொதுவில் வெளியிடப்படுகிறது.



கூடுதல் தீச்சுவராக, ஒவ்வொரு பரிமாற்றத்திற்கும் ஒரு புதிய இணைத் திறவியை பயன்படுத்துவது மூலம், பொதுவான உரிமையாளர் இணைப்பிலிருந்து பாதுகாக்க முடியும். ஆனால் பல உள்ளீடுகளுடன் கூடிய பரிமாற்றங்களின் சில இணைப்புகளைத் தவிர்க்க முடியாது, மேலும் அவற்றின் உள்ளீடுகளானது, அவைகள் ஒரே உரிமையாளருக்குச் சொந்தமானவை என்பதை கட்டாயம் வெளிப்படுத்தும். ஒரு திறவியின் உரிமையாளரை வெளிப்படுத்துவது ஆபத்தாகும், மேலும் இணைப்பானது அதே உரிமையாளரின் மற்றப் பரிமாற்றங்களையும் வெளிப்படுத்தலாம்.

11. கணக்கீடுகள்

நாம் கருதும் சூழ்நிலைக்காட்சியில், தாக்குபவர் ஒருவர், நேர்மையானச் சங்கிலித்தொடரை விட வேகமான ஒரு மாற்றுச் சங்கிலித்தொடரை உருவாக்க முயலுகிறார். இது நிறைவேற்றப்பட்டாலும் கூட, ஒன்றுமில்லாமல் மதிப்பை உருவாக்குவது அல்லது தாக்கியவருக்கு சொந்தமில்லாத பணத்தை எடுத்துக்கொள்வது, போன்ற தன்னிச்சையான மாற்றங்களைச் செயல்படுத்த அமைப்பை பயன்படுத்த முடியாது. கணினிமுனைகளானது செல்லாதப் பரிமாற்றத்தை கட்டணமாக ஏற்கப் போவதில்லை, மேலும் அவற்றைக் கொண்டிருக்கும் ஒரு தொகுதியை, நேர்மையான கணினிமுனைகள் ஒருபோதும் ஏற்றுக்கொள்ளாது. தாக்குபவர் ஒருவர், அவர் அண்மையில் செலவழித்தப் பணத்தை திரும்ப எடுக்க, தனது சொந்த பரிமாற்றம் ஒன்றை மட்டுமே மாற்ற முயற்சிக்க முடியும்.

நேர்மையானச் சங்கிலித்தொடருக்கும் மற்றும் தாக்குபவர் சங்கிலித்தொடருக்கும் இடையிலான போட்டியை, ஈருறுப்பு சீரற்ற நடை மூலம் வகைப்படுத்த முடியும். வெற்றி நிகழ்வு என்பது, நேர்மையானச் சங்கிலித்தொடரை கூடுதலான ஒரு தொகுதி மூலம் நீட்டித்து, அதனுடைய தலைமையை +1 ஆல் அதிகரிப்பது, மேலும் தோல்வி நிகழ்வு என்பது, தாக்குபவருடையச் சங்கிலித்தொடரை கூடுதலான ஒரு தொகுதி மூலம் நீட்டித்து, அதனுடைய இடைவெளியை −1 ஆல் குறைப்பது.

தாக்குபவர் ஒருவரிடம் வழங்கப்பட்ட பற்றாக்குறையிலிருந்து, ஈடுகொடுத்துப் பிடிக்கும் நிகழ்தகவை கேம்ப்ளர்'ஸ் ரூயின் சிக்கலுக்கு ஒப்பிடலாம். வரம்பில்லா கடன் பெற்ற சூதாட்டக்காரர் ஒருவர் பற்றாக்குறையில் தொடங்குகிறார் என்று வைத்துக்கொள்வோம், மேலும் அவர் சமநிலையை அடையும் முயற்சியில், எண்ணற்ற சோதனைகளில் திறமையாக விளையாடி ஆகவேண்டும். அவர் எப்போது சமநிலையை அடைவார், அல்லது ஒரு தாக்குபவர் எப்போது நேர்மையானச் சங்கிலித்தொடருக்கு ஈடுகொடுத்து அதைப் பிடிப்பார் என்பதன் நிகழ்தகவை நம்மால் கணக்கிடமுடியும், பின்வருமாறு [8]:

p = ஒரு நேர்மையானக் கணினிமுனை அடுத்தத் தொகுதியை கண்டறியும் நிகழ்தகவு.
q = தாக்குபவர் அடுத்தத் தொகுதியை கண்டறியும் நிகழ்தகவு.
q_z = z தொகுதிகள் பின்னால் இருக்கும் தாக்குபவர், எப்போது ஈடுகொடுத்து பிடிப்பார் என்பதன் நிகழ்தகவு.

$$q_z = \begin{cases} 1 & \text{if } p \leq q \\ (q/p)^z & \text{if } p > q \end{cases}$$

நம்முடையக் கருதுகோளின்படி $p > q$, தாக்குபவர் அடையவேண்டியத் தொகுதிகளின் எண்ணிக்கை அதிகரிப்பைப் பொறுத்து, இந்த நிகழ்தகவானது அடுக்கேற்ற முறையில் குறைகிறது. அவருக்கு எதிரான தடைகளுடன், ஆரம்பத்திலேயே அதிர்ஷ்ட வசமாக அவர் முன்னோக்கிச் செல்லவில்லை என்றால், அவரது வாய்ப்புகளானது மறையும் அளவுக்குச் சிறிதாகி மேலும் கூடுதலாகப் பின்தங்குகிறார்.

நாம் இப்போது கருத்தில் கொள்ளவேண்டியது, இனி அனுப்புநரால் பரிமாற்றத்தை மாற்றவே முடியாது என போதுமான உறுதியுடன் இருப்பதற்கு முன், புதிய பரிமாற்றத்தைப் பெறுபவர் எவ்வளவு காலம் காத்திருக்க வேண்டும். இங்கு அனுப்புநரை நாம் தாக்குபவர் என்று கொள்கிறோம், அவர் பெறுநருக்கு பணம் செலுத்தியதை சிறிது காலத்திற்கு நம்ப வைக்க விரும்புகிறார், பின்னர் சிறிது காலம் கழித்து அதை மாற்றி தனக்கே திருப்பிச் செலுத்திக்கொள்கிறார். இது நிகழும்போது பெறுநருக்கு எச்சரிக்கை செய்யப்படும், ஆனால் அனுப்புநர் இதை மிகவும் தாமதமான ஒரு நிகழ்வாக நம்புகிறார்.

பெறுநர் ஒரு புதிய இணைத் திறவியை உருவாக்குகிறார், மேலும் கையொப்பமிடுவதற்கு சற்று முன் அனுப்புநருக்கு அந்த பொதுத் திறவியை கொடுக்கிறார். இது அனுப்புநரை, அதன் மீது தொடர்ந்து வேலை செய்து, போதுமான அளவு முன்னேறுவதற்கான அதிர்ஷ்டத்தை அடைந்தவுடன், அக்கணமே அந்தப் பரிமாற்றத்தை செயல்படுத்தி, முன்கூட்டியே தொகுதிகளின் சங்கிலியை தயாரிப்பதில் இருந்து தடுக்கிறது. ஒருமுறை பரிமாற்றம் அனுப்பப்பட்டதும், நேர்மையற்ற அனுப்புநர், அவரது மாற்றுப் பதிப்புள்ள பரிமாற்றத்தின் ஒரு இணைச் சங்கிலித்தொடரின் மீது ரகசியமாக வேலை செய்யத் தொடங்குகிறார்.

ஒரு தொகுதியில், பரிமாற்றமானது சேர்க்கப்படும் வரை பெறுநர் காத்திருக்கிறார், மேலும் z தொகுதிகளானது அதன் பின்னால் இணைக்கப்படுகிறது. தாக்குபவரால் செய்துமுடிக்கப்பட்ட முன்னேற்றத்தின் அளவானது அவருக்கு தெளிவாகத் தெரியவில்லை, ஆனால் ஒரு தொகுதிக்கு சராசரியாக எதிர்பார்க்கப்படும் நேரத்தை, நேர்மையானத் தொகுதிகள் எடுத்ததாகக் கருதிக் கொள்கின்றார், தாக்குபவரின் முன்னேற்றத் திறனானது எதிர்பார்க்கப்படும் மதிப்புடன் கூடிய ஒரு பாய்ஸான் பரவலாக இருக்கும்:

$$\lambda = z\frac{q}{p}$$

நிகழ்தகவைப் பெறுவதற்கு தாக்குபவரால் இப்போதும் ஈடுகொடுக்கமுடியும், அவர் அந்த புள்ளியில் இருந்து ஈடுகொடுத்து, நிகழ்தகவால் அடைய முடிந்த முன்னேற்றத்தின் ஒவ்வொரு அளவுடனும், நாம் பாய்ஸான் அடர்த்தியைப் பெருக்குகிறோம்:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \begin{cases} (q/p)^{(z-k)} & if\ k \le z \\ 1 & if\ k > z \end{cases}$$

பரவலின் முடிவில்லா வாலின் கூட்டலைத் தவிர்க்க மறுசீரமைக்கப்படுகிறது...

$$1 - \sum_{K=0}^{Z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

C குறியீட்டிற்கு மாற்றப்பட்டுள்ளது...

```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
         double poisson = exp(-lambda);
         for (i = 1; i <= k; i++)
             poisson *= lambda / i;
         sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

சில முடிவுகள், நிகழ்தகவானது z உடன் அடுக்கேற்றமாக குறைவதை நம்மால் பார்க்கமுடிகிறது.

```
q=0.1
z=0     P=1.0000000
z=1     P=0.2045873
z=2     P=0.0509779
z=3     P=0.0131722
```

z=4 P=0.0034552
z=5 P=0.0009137
z=6 P=0.0002428
z=7 P=0.0000647
z=8 P=0.0000173
z=9 P=0.0000046
z=10 P=0.0000012

q=0.3
z=0 P=1.0000000
z=5 P=0.1773523
z=10 P=0.0416605
z=15 P=0.0101008
z=20 P=0.0024804
z=25 P=0.0006132
z=30 P=0.0001522
z=35 P=0.0000379
z=40 P=0.0000095
z=45 P=0.0000024
z=50 P=0.0000006

P க்கு 0.1% க்கும் குறைவான தீர்வு...

P < 0.001
q=0.10 z=5
q=0.15 z=8
q=0.20 z=11
q=0.25 z=15
q=0.30 z=24
q=0.35 z=41
q=0.40 z=89
q=0.45 z=340

12. முடிவுரை

நாம் நம்பிக்கைச் சாராத மின்னணுசார் பரிமாற்றங்களுக்கான அமைப்பு ஒன்றை முன்மொழிகிறோம். டிஜிட்டல் கையொப்பங்களால் செய்யப்பட்ட நாணயங்களின் வழக்கமான கட்டமைப்புடன் அதை நாம் தொடங்கினோம், இது வலுவானக் கட்டுப்பாட்டுடன் கூடிய உரிமையை வழங்குகிறது, ஆனால் இரட்டைச் செலவுகளைத் தடுக்க ஒரு வழியின்றி போனால் இது முழுமையடையாது. இந்த தீர்வுக்கு, ப்ரூஃப்-ஆஃப்-வொர்க்கைப் பயன்படுத்தி, பரிமாற்றங்களின் பொது நிகழ்ச்சிக்கோவையைப் பதிவு செய்யும், ஒரு பியர்-டு-பியர் வலையமைப்பை நாம் முன்மொழிந்தோம், இதன் பெரும்பான்மை கணினித் திறன்கள் நேர்மையானக் கணினிமுனைகளால் கட்டுப்படுத்தப்படும் வரை, தாக்குபவர்களால் கணக்கீட்டு ரீதியாக மாற்றம் செய்ய நடைமுறைச் சாத்தியமற்றதாக விரைவில் மாற்றப்படுகிறது. இந்த வலையமைப்பானது அதன் கட்டமைப்பற்ற எளிமையால் வலுவாக இருக்கிறது. எல்லாக் கணினிமுனைகளும் சிறிய ஒருங்கிணைப்புடன் ஒன்றாக வேலை செய்கிறது. அவைகளை அடையாளம் காண வேண்டிய அவசியமில்லை, ஏனென்றால் செய்திகள் எந்த ஒரு குறிப்பிட்ட இடத்திற்கும் வழிப்படுத்தப்படாமல், சிறந்த முயற்சியின் அடிப்படையில் மட்டுமே அவைகள் வழங்கப்படுகின்றன. கணினிமுனைகள் தங்கள் விருப்பப்படி வலையமைப்பிலிருந்து வெளியேறி மீண்டும் இணையலாம். வெளியேறியபோது நடந்த மாற்றங்களை மீண்டும் புதுப்பிக்க, மிக நீளமான ப்ரூஃப்-ஆஃப்-வொர்க் சங்கிலித்தொடரைச் சான்றாக ஏற்றுக்கொள்கிறது. அவைகள் தங்கள் கணினித் திறனுடன் வாக்களிக்கிறது, சரியான தொகுதிகளின் மீது வேலை செய்து நீட்டிப்பதன் மூலம் தங்கள் ஏற்பை வெளிப்படுத்துகிறது, மேலும் தவறான தொகுதிகளின் மீது வேலை செய்ய மறுப்பதன் மூலம் தங்கள் நிராகரிப்பை வெளிப்படுத்துகிறது. ஒருமித்த இயக்கமுறையைப் பயன்படுத்தி தேவையான விதிகளையும் மற்றும் ஊக்கத்தொகைகளையும் செயற்படுத்த முடியும்.

குறிப்புகள்

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In *20th Symposium on Information Theory in the Benelux*, May 1999.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," *In Journal of Cryptology*, vol 3, no 2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," *In Sequences II: Methods in Communication, Security and Computer Science*, pages 329-334, 1993.

[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," *In Proceedings of the 4th ACM Conference on Computer and Communications Security*, pages 28-35, April 1997.

[6] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," *In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society*, pages 122-133, April 1980.

[8] W. Feller, "An introduction to probability theory and its applications," 1957.