Freeman குடும்பம்

ஜூலை 4, 2019

EPIC CASH

EPIC PRIVATE INTERNET CASH
காவிய தனியார் இணைய பணம்

ஒரு பியர்-டு-பியர் மின்னணு பண அமைப்பு

சேமிப்பின் மதிப்பு + பரிமாற்ற ஊடகம் + கணக்கீடு அலகு

உலகளாவிய நிதி அமைப்புக்கான அணுகல் 1.7 பில்லியன் பெரியோர்களுக்கு இல்லை, மேலும் 1.3 பில்லியனுக்கு குறைவான அணுகல் உள்ளது. Epic Cash உலக சந்தையில் தனிநபர்களை இணைப்பதன் மூலம் மனித ஆற்றலை வெளிப்படுத்தும். வேகமாகவும், உண்மையிலே இலவசமாக பயன்படுத்தவும், அனைவருக்கும் திறந்திருக்கும்.

Version 7.1b Tamil

உள்ளடக்கம்

I. சுருக்கம்

Epic Cash-ஆனது உண்மையான P2P இனைய பணத்தை நோக்கிய பயணத்தின் இறுதி புள்ளி, தனியார் நிதியமைப்பின் மூலைகல். Epic நாணயமானது உலகின் மிகச்சிறந்த தனிமறைப்பு-பாதுகாக்கும் இலக்கமுறை பணமாக மாறும் நோக்கம் கொண்டுள்ளது. இந்த இலக்கை நிறைவேற்றும் பொருட்டு, பணத்தின் மூன்று முக்கிய செயல்பாடுகளை அது பூர்த்தி செய்கிறது:

1. **சேமிப்பின் மதிப்பு** - சேமிக்கலாம், மீட்டெடுக்கலாம், பிற்காலத்தில் பரிமாறிக்கொள்ளலாம், மீட்டெடுக்கும்போது கணிக்கக்கூடிய மதிப்புடையது;
2. **பரிமாற்ற ஊடகம்** - மதிப்பின் தரத்தை குறிப்பதாகவும், பொருட்கள் அல்லது சேவைகளுக்கு பரிமாற்றவும் ஏற்றுக்கொள்ளப்படுபவை;
3. **கணக்கீடு அலகு** - ஒரு பொருளின் மதிப்பு கணக்கிடப்பட்டு ஒப்பிடப்படும் அலகு

	$ USD	BTC	EPIC
சேமிப்பின் மதிப்பு	✗	✓	✓
பரிமாற்ற ஊடகம்	✓	✗	✓
கணக்கீடு அலகு	✓	✗	✓

2009 ஆம் ஆண்டில் Bitcoin பிளாக்செயின் அடிப்படையிலான முதல் இலக்கமுறை நாணயமாக உருவெடுத்தது, அதன் மூன்று வரையறுக்கும் பண்புகளைக் கொண்டு மற்ற மறைகுறியீட்டுநாணயங்கள் மதிப்பீடு செய்யப்படும்:

- **நம்பிக்கையின்மை** - யாரும் பிணையம் செயல்பட எந்தவொரு மையப்படுத்தப்பட்ட நிறுவனத்தையோ அல்லது எதிர் தரப்பினரையோ நம்ப தேவையில்லை;
- **மாறாத்தன்மை** - பரிவர்த்தனைகள மாற்றிச் செயல்படுத்த முடியாது.
  a. வரலாற்றை திரும்ப எழுதுவது மிகவும் சாத்தியமற்றதாக்கேவா அல்லது கடினமாகேவா இருக்க வேண்டும்;
  b. ஒரு தனியார் விசையுடன் தொடர்பு உடைய நிதியை நகர்த்துவது அந்த தனியார் விசையின் உரிமையாளரைத் தவிர வேறுயாராலும் இயலாது;
  c. அனைத்து பரிவர்த்தனைகளும் பிளாக்செயினில் பதிவு செய்யப்படும்
- **பரவலாக்கம்** - "பிளாக்செயின்கள் அரசியல் ரீதியாக பரவலாக்கப்பட்டவை (அவற்றை யாரும் கட்டுப்படுத்தாவில்லை) மேலும் கட்டமைப்பு ரீதியாகவும் பரவலாக்கப்பட்டவை (உள்கட்டமைப்பில் எங்கும் செயலிழப்பு இல்லை) ..."[1].

Bitcoin அதன் பணக்கொள்கையின் கட்டைமப்பில், காலத்தால் சோதிக்கப்பட்ட அடிப்படைகளை கைடபிடிக்கும் போது தொழில்நுட்ப ரீதியாக புதிய தடங்களை உருவாக்கியது. Bitcoin-னின் ெ வற்றி நம்பகமான, மாறாத, பரவலாக்கப்பட்ட பிளாக்செயினுடன் இணைந்து அதன் வைரயறுக்கப்பட்ட வழங்கீடுடன் வலுவான ெ தாடர்புடையது. Epic Cash ஆனது பணவீக்கத்தைக் குறைக்கும் Bitcoin-னின் பணக்கொள்கையயும் வைரயறுக்கப்பட்ட வழங்கீட்டையும் முன்மாதிரியாக கொண்டு Epic நாணயத்தை மதிப்புள்ள சேமிப்பாக செயல்பட முடியும் என்பைத உறுதிப்படுத்துகிறது.

Bitcoin வெற்றியைடந்தேபாதிலும், 10 ஆண்டுகளுக்கு முன் அது தொடங்கியதிலிருந்து சில குறைபாடுகள் வெளிப்பட்டுள்ளன. பிற திட்டங்கள் இந்த குறைபாடுகளை சமாளிக்க முயற்சித்தன, இவற்றில் சிறந்தவற்றை எங்கள் தொடக்க புள்ளியாக பயன்படுத்த நாங்கள் ஆராய்ந்தோம். கடுமையாக ெவன்ற சாதைனகளையும் Epic Cash-ன் முன்னோடிகளின் தவறுகளை கண்டுடறியவும் எங்களுக்கு உதவ, Grin-னின் குறியீடு மற்றும் பல திட்டங்களின் சிறந்த பணிகளைப் பயன்படுத்த முடிவு செய்தோம். Epic Cash ஒரு சிறந்த நாணயதிற்குள்ள முக்கிய குணங்களை கொண்டுள்ளது:

- **அழிமாற்றத்தன்மை** - ஒரு Yen அல்லது Yuan எப்பொழுதும் சமமாக இருப்பதோடு, மற்றொரு Yen அல்லது Yuan-னுடன் மாற்றத்தக்கது போல, கொடுக்கப்பட்ட Epic-யின் மதிப்பு எப்போதுமே Epic-யின் மற்றொரு அலகுக்கு சமமாக இருக்க வேண்டும். அழிமாற்றுத்தன்மையை அடைவது பெருமளவில் தனிமறைபுடன் பிணைந்திருக்கும்.
- **அளவிடுதல்** - Epic Cash ஆனது திறைமயான இடஒதுக்கீடுள்ள பிளாக்செயினை பராமரிக்கிறது, அதன் மீது வளம்-செறிந்த உபகரணங்கள் இல்லாமல் புதிய முனைகைள எளிதாக நிறுவ முடியும். Epic Cash பிளாக்செயின், Bitcoin-னின் செய்வீதத்தை விட, குறைந்தது இரண்டு மடங்கு திறன் கொண்டது.
- **தனிமைறபு** - மூன்றாம் தரப்பினரிடமிருந்து பரிவர்த்தனைகளின் விவரங்களை பாதுகாப்பதன் மூலம் Epic வைத்திருப்பவர்கள் மற்றும் பயனர்களின் அநாமதேயத்தை Epic Cash பிளாக்செயின் பாதுகாக்கிறது, மேலும் இது கண்காணிக்க மற்றும் கண்டறிய இயலாதவாறு வடிவமைக்கப்பட்டுள்ளது.
- **வேகம்** - Epic Cash பரிவர்த்தனைகள் மென்மையாக, தொடர்ச்சியாக மேலும் முந்தைய தலைமுறை பிளாக்செயின் தொழில்நுட்பத்தை விட மிக வேகமாக செயல்படுகின்றன. முழுமையான பரிவர்த்தனை உறுதிப்பாட்டை அடைய Bitcoin-னுக்கு ஆறு 10 நிமிட தொகுதிகள் தேவைப்படும் நிலையில், Epic பரிவர்த்தனைகள் 1 நிமிட தொகுதி மைன் செய்யப்பட்டவுடன் ஒரு தொகுதி உறுதிப்படுத்தலுக்குள் நிகழ்கின்றன.

[1] **Buterin, Vitalik, The Meaning of Decentralization, 6 February, 2017,** https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

II. தனிமறைபு

நவீன கால பணத்தைப் பயன்படுத்துவது மக்களுக்கும் நிறுவனங்களுக்கும் இடையிலான கணக்கீடு அலகுகளின் கூட்டு பரிமாற்றம் என புரிந்து கொள்ளலாம். எந்த நேரத்திலும் பணத்தின் இயற்கையை பின்வரும் கேள்விகளுக்கு பதிலளிப்பதன் மூலம் படமாக்கலாம்:

1. *யார் அதை வைத்திருக்கிறார்கள், அவர்கள் எவ்வளவு வைத்திருக்கிறார்கள்?*
2. *யார் யாருடன் பரிவர்த்தனை செய்கிறார்கள், அது எவ்வளவு?*

பாரம்பரிய ஃபியட் நாணயங்களுக்கும், உண்மையில் பிட்காயினுக்கும், அந்த கேள்விகளுக்கு நாம் பதிலளிக்க முடியும். அவ்வாறு செய்யும்போது, நுகர்வு முறைகள், உரிமை மற்றும் பரிவர்த்தனை சகாக்கள் போன்ற மக்களின் வாழ்க்கையைப் பற்றி அதிகம் வெளிப்படுத்தலாம். மதிப்பின் பரிமாற்றங்களைக் கண்டறிவதன் மூலம் ஒரு நபரின் ஆர்வங்கள் மற்றும் நோக்கங்களைப் பற்றி மிகவும் துல்லியமான முடிவுகளை எடுக்க முடியும். தனிமறைபு இல்லையென்றால், பரிவர்த்தனை தரவுகள் சூறையாடும் மூன்றாம் தரப்பினரின் கைகளில் ஆபத்தான தகவலாக அமையும்.

கடந்த பத்தாண்டுகளில் மறைகுறியீட்டு நாணயத்தின் பயன்பாடு மாறுபட்ட பிளாக்செயின் செயலாக்கங்களில் "தனிமறைபு" தொடர்ச்சியைக் காட்டுகிறது. தனிமறைபு அளவுகோலை கருத்தில் கொள்ள வேண்டும்மென்றால், ஒரு முனையில் திறந்ததும் இழிவானதும் மறுபுறம் அநாமதேயமும் வரம்புகளாக கொண்டது. தனிமறைபு அரிந்துவிடுகையில், மறைகுறியீட்டு நாணயத்தின் ஒரு அத்தியாவசிய மூலைக்கலான, நம்பிக்கையின்மை, குறைகிறது. Bitcoin பிளாக்செயின் பகுப்பாய்வு சேவைகளின் வெற்றிக்கு சான்றாக, Bitcoin தனிமறைபு ஸ்பெக்ட்ரமின் படுபயங்கர வெளிப்படையான முனையில் அமைந்துள்ளது. பயனர்கள் கறைபடிந்த Bitcoin-னில் கவனக்குறைவாக பரிவர்த்தனைகள் செய்யக்கூடாது என்பதை உறுதிப்படுத்த அதிகளவிலான நடவடிக்கைகளை எடுக்க வேண்டும். Epic Cash-யின் தீர்வு அநாமதேயத்தை நோக்கி ஊசலாடுகிறது, தனிநபரின் தனிமறைபு மற்றும் பரிவர்த்தனைகளின் தனிமறைபு ஆகிய இரண்டையும் அமைப்பின் ஒரு அடிப்படை மட்டத்தில் பொறியாக்கம் செய்யப்படுவைத உறுதி செய்வதன் மூலம் இந்த அத்தியாவசிய பண்பை மீட்டெடுக்கிறது.

அடையாளத்தின் தனிமறைபு

பரிவர்த்தனையின் தனிமறைபு

அடையாளத்தின் தனிமறைபு

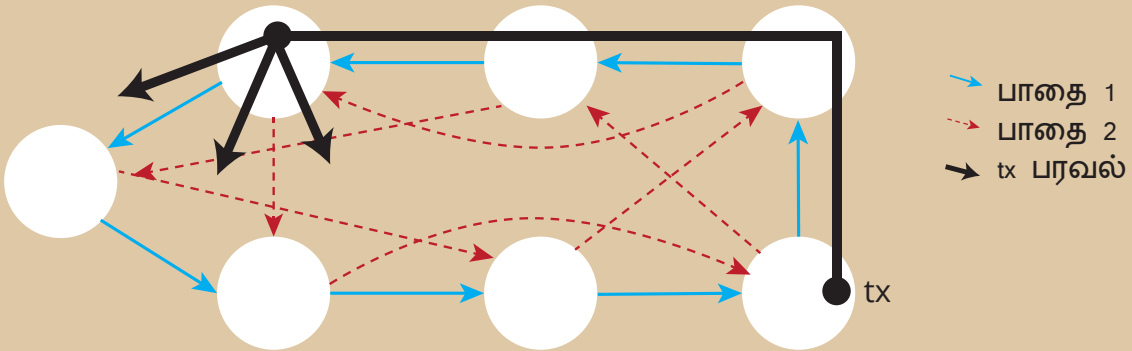
Bitcoin போன்ற பெரும்பாலான மறைகுறியீட்டுநாணயங்கள் வாலட்-இல் சேமிக்கப்படுகின்றன, அதன் முகவரிகள் வாலட்-இன் தனியார் விசையிலிருந்து தருவிக்கப்பட்ட பொது விசையை குறிக்கின்றன. இந்த முகவரிகள் இலக்கமுறை உலகில் ஒருவரின் தனிப்பட்ட பெட்டகத்தின் இடங்காட்டியாக கருதலாம். Epic Cash பிளாக்செயின் முகவரிகளை நீக்குகிறது மேலும் அதற்கு பதிலாக அனைத்து பொது மற்றும் தனியார் விசைகளுக்கு ஒரே பயன்பாட்டு அடிப்படையில் ஒரு பெரிய MultiSignature- ஐ பயன்படுத்துகிறது.

Bitcoin வாலட் முகவரிகள் இலக்கமுறை உலகில் ஒரு பெட்டகத்தின் இடம்காட்டியாக இருப்பதால், அந்த வாலட்-ஐ உரிமையாளரின் இணைய நெறிமுறை (IP) முகவரியில் காணலாம், இது ஒரு குறிப்பிட்ட நேரத்தில் உரிமையாளரை ஒரு தனித்துவமான இடத்தில் உள்ள கணினியோடு இணைகிறது. எளிமையாக விளக்கினால்: ஒரு Bitcoin பரிவர்த்தனை நடைபெறும் போது, பரிவர்த்தனையை ஒரு 'முனை' எனப்படும் தகவல்தொடர்பு மையத்திலிருந்து ஒளிபரப்பப்பட்டு பின்னர் 'பியர்ஸ்' எனப்படும் பிற முனைகளுக்கு கடத்தப்படுகிறது. அந்த தகவல் முழு பிணையத்திலுள்ள ஒவ்வொரு முனைகளுக்கும் தொடர்ச்சியாக விரைவாக பரவுகிறது. இந்த செயல்முறைக்கு "Gossip நெறிமுறை" என்று பெயரிடப்பட்டுள்ளது. மிகவும் எளிமையாக, ஒவ்வொரு Bitcoin-னுக்கும் அதன் ஆன்லைன் நிலை புலப்படும் மேலும் அதன் இருப்பிடம் அல்லது அதற்கு பதிலாக Bitcoin-னின் உரிமையாளரின் இருப்பிடம் கண்டறியக்கூடம். பத்திரிகையாளர் Grace Caffyn குறிப்பிட்டுள்ளபடி, Bitcoin "வீட்டு இணைய இணைப்பிலிருந்து கூகிள் தேடலை பயன்படுத்துவதை விட ரகசியமல்ல"[2].

வாலட் முகவரிகளை நீக்குவதோடு, IP முகவரிகளைக் கண்டுடறியாதவாறு உறுதி செய்வதன் மூலம் Epic Cash பிளாக்செயின் அடையாளத்தின் தனிமறைபை பாதுகாக்கிறது. Dandelion++ நெறிமுறையினை ஒருங்கிணைப்பதன் மூலம் இதைச் செய்கிறது. Dandelion++ நெறிமுறை அதன் முன்னோடியான அசல் Dandelion நெறிமுறையை மேம்படுத்தி, பிளாக்செயினில் டிஅனோனிமைசேஷன் தாக்குதல்களை எதிர்க்க ஏழு ஆராய்ச்சியாளர்களின் தொடர்ச்சியான பணியின் விளைவாகும். Dandelion++ மூலம், பரிவர்த்தனைகள் சீரற்ற பின்னிப் பிணைந்த பாதைகள் அல்லது 'கேபிள்கள்' வழியாக அனுப்பப்படுகின்றன, பின்னர் ஒரு Dandelion பூவின் காய்களை தண்டுகளிலிருந்து ஊதப்படுவது போல, திடீரென ஒரு பெரிய முனைகளின் பிணையத்திற்கு பரப்புகின்றன (படம் 1). இது பரிவர்த்தனைகள் மற்றும் IP முகவரிகளை அவற்றின் தோற்றத்திற்குத் பின்தொடர கிட்டத்தட்ட சாத்தியமற்றது.

படம் 1: Dandelion++ நெறிமுறையுடன் பரிவர்த்தனைகளை அநாமேதயமாக்குதல்.

Dandelion++ 4-வழக்கமான வரைபடத்தில் இரண்டு பின்னிப்பிணைந்த பாதைகளில் ஒன்றின் வழியாக செய்திகளை அனுப்புகிறது, பின்னர் பரவலைப் பயன்படுத்தி ஒளிபரப்பப்படுகிறது. படத்தில், பரிவர்த்தனை நீல திட பாதை மீது கடத்தப்படுகிறது[3]. இந்த செயல்முறை பரிவர்த்தனைகளின் மூலத்தை கண்டுபிடிப்பதை கடினமாக்குகிறது, இதனால் தனிமறைபு பாதுகாக்கப்படுகிறது.



[2] F2Caffyn, Grace, *Chainalysis CEO Denies 'Sybil Attack' on Bitcoin's Network,* 14 மார்ச், 2015, https://www.coindesk.com/chainalysis-ceo-denies-launching-sybil-attack-on-bitcoin-network

[3] Fanti, G, Venkatakrishnan, S B, Bakshi, S, Denby, B, Bhargava, S, Miller, A & Viswanath, P 2018, 'Dandelion++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees', *Proc. ACM Meas. Anal. Comput. Sys.*, Vol. 2, Article 29, pg. 8, https://www.readkong.com/page/dandelion-lightweight-cryptocurrency-networking-with4805755-?p=1

பரிவர்த்தனையின் தனிமறைபு

Epic Cash பிளாக்செயின் பரிவர்த்தனை தனிமறைபை பரிவர்த்தனையின் அளவுகள் மற்றும் அனுப்புநர்-பெறுநர் உறவை மறைப்பதன் மூலம் உறுதிப்படுத்துகிறது. Gregory Maxwell (Bitcoin Core நிரலர், Blockstream-இன் இணை-நிறுவனர் மற்றும் CTO) உருவாக்கிய முறைகளான, ரகசிய பரிவர்த்தனைகள் (CT)[4] மற்றும் CoinJoin[5] ஆகியவற்றிலுள்ள பழக்கமான யோசனைகளைப் பயன்படுத்துவதன் மூலம் இது அடையப்படுகிறது

CT, முதலில் Adam Back-ஆல் உருவாக்கப்பட்டது, பின்னர் Maxwell-ஆல் மேன்மைப்படுத்தப்பட்டது, இது Homomorphic மறையக்கத்தின் மூலம் பரிவர்த்தனைகளை சிறிய பகுதிகளாக உடைத்து செயல்படுகிறது, இது தனிமறைபை பாதுகாக்க முதலில் மறைக்கப்பட்ட தகவல்களைக் மறைவிலக்கம் செய்யாமல் கணக்கிடுகிறது. ஒருமுறை பிரிக்கப்பட்டால், அந்த துண்டுகளின் மதிப்பை மறைக்க பரிவர்த்தனை துண்டுகளின் கலவையில் சீரற்ற எண்களை வீசும் அமைப்பு, மறைக்கும் காரணிகள் ஆகும், இவற்றால் பரிவர்த்தனைகளின் உண்மையான அளவுகளை பார்வையாளர்களால் பார்க்க முடியாது, இறுதியில், பரிவர்த்தனை செய்யும் தரப்பின்னர்களுக்கு மட்டுமே ஒரு பரிமாற்றத்தின் மதிப்பு தெரியும், அதே சமயம் வெளியீட்டு மதிப்புகளின் கூட்டுத்தொகை உள்ளீட்டு மதிப்புகளின் கூட்டுத்தொகைக்கு சமம் என்பதை உறுதிப்படுத்துவதன் மூலம் பரிவர்த்தனை பிணையத்தால் சரிபார்க்கப்படுகிறது, மேலும் வெளியீட்டு மறைக்கும் காரணிகளின் கூட்டுத்தொகை உள்ளீட்டு மறைக்கும் காரணிகளின் கூட்டுத்தொகைக்கு சமம்.

இவற்றை மேலும் சிக்கலாக்குவதற்கு, அனைத்து Epic Cash பரிவர்த்தனைகளும் CT-யால் மூடப்பட்டிருக்கும், பின்னர் அவை ஒன்றிணைந்து பரிவர்த்தனை செய்யும் தரப்பினருக்கு இடையிலான தொடர்புகளை மறைக்கின்றன. இது Maxwell-லின் இரண்டாவது கருத்தான CoinJoin மூலம் செயல்படுத்தப்படுகிறது.

CoinJoin-ஐ எளிமையாக விளக்குவதற்கு, A, B மற்றும் C ஆகியவை முறையே X, Y மற்றும் Z க்கு Epic-ஐ அனுப்புகின்றன என கொள்ளுங்கள். CoinJoin ஊடகம் மூலம் அனுப்பப்படுவதில், அறியப்பட்டவை அனைத்தும் A, B மற்றும் C ஆகியவை அனுப்புகின்றன, X, Y மற்றும் Z ஆகியவை பெறுகின்றன, அதே ே நரத்தில் பரிவர்த்தைனத் ெ தாகைகள் அறியப்படுவதில்லை. Epic Cash-ற்கு CoinJoin அமைப்பானது One-Way Aggregate Signatures (OWAS) மூலம் அடிப்பைடையாகும், இது ஒரு பிளாக்கிற்குள் உள்ள அனைத்து பரிவர்த்தனைகளையும் ஒரே பரிவர்த்தனையாக இணைக்கிறது.

தனிமறைபு: சுருக்கம்

Epic Cash பிளாக்செயின் தனிநபர்களின் தனிமறைபையும் அவர்களின் பரிவர்த்தனைகளையும் கீழ்கண்டவாறு பாதுகாக்கிறது:

- **வாலட் முகவரிகளை நீக்குதல் - பிளாக்செயினுக்குள் உள்ள இலக்கமுறை பெட்டகத்திற்கான இடம்காட்டிகள் எதுவும் இல்லை. பரிவர்த்தனைகள் ஒரு நபரிலிருந்து இன்னொரு நபருக்கு, ஒரு வாலட்டிலிருந்து இன்னொரு வாலட் என்னும் அடிப்படையை கொண்டு கட்டமைக்கப்படுகின்றன;**
- **Dandelion++ நெறிமுறை - பரிவர்த்தைன அனுப்புநரின் IP முகவரியிலிருந்து அப்பரிவர்த்தனையின் இலக்கமுறை பாதைவழிகளை மைறக்கிறது;**
- **ரகசிய பரிவர்த்தைனகள் - பரிவரபரிவர்த்தனைகளை பல துண்டுகளாகப் பிரித்து, அந்த துண்டுகளின் சேகரிப்பில் மறைக்கும் காரணிகளை அறிமுகப்படுத்தி, அதனால் துண்டுகளின் மதிப்புகள் மற்றும் பிற பரிவர்த்தனை அளவுருக்களை அறிய வாய்ப்பில்லை;**
- **CoinJoin - பரிவர்த்தைனகைள மூட்டைகளாக இணைத்து பரிவர்த்தைன செய்யும் தரப்பினருக்கு இடையிலான உறைவ மைறக்கிறது.**

[4] Maxwell, Gregory, ***Confidential Transactions,*** Technical Report (2015), https://people.xiph.org/~greg/confidential_values.txt

[5] Maxwell, Gregory, ***CoinJoin: Bitcoin Privacy for the Real World***, 22 August, 2013, post on Bitcoin Forum, https://bitcointalk.org/index.php?topic=279249.0

III. அழிமாற்றத்தன்மை

Litecoin-ஐ உருவாக்கிய Charlie Lee, Bitcoin மற்றும் Litecoin-னில் பணத்திற்கு உண்டான பண்புகளில் இல்லாத ஒரே பண்பு அழிமாற்றத்தன்மை என்று கூறினார், அந்த நாணயங்களுக்கான அடுத்த போர்க்களமாக தனிமறைபும் அழிமாற்றத்தன்மையும் இருப்பதாக ஒப்புக் கொண்டார்[6]. உலகின் முன்னணி பிளாக்செயின் நிபுணர்களில் ஒருவரான Andreas Antonopoulos, "...கறைபடிந்த நாணயங்கள் அழிவுகரமானவை. நீங்கள் அழிமாற்றத்தன்மை மற்றும் தனிமறைபு ஆகியவற்றை உடைத்தால், நீங்கள் நாணயத்தை உடைக்கிறீர்கள்." என்று கூறினார்[7].

அழிமாற்றத்தன்மை என்பது பொருட்கள் அல்லது சொத்துகளின் தொகுப்பின் பண்பாகும், அந்த தொகுப்பின் தனிப்பட்ட அலகுகள் சம மதிப்பு மற்றும் ஒன்றுக்கொன்று மாறக்கூடியவை என்பதை உறுதி செய்கிறது. இதுவே நாணயத்தின் ஆரம்பகால வடிவங்களை அவற்றின் முந்தைய பண்டமாற்று முறைகளிலிருந்து வேறுபடுத்துகிறது. பணத்தின் அழிமாற்றத்தன்மையின் மீது நம்பிக்கை இல்லையென்றால், அந்த பணம் விரைவாக அதன் பயன்பாட்டை இழக்கிறது. கீழே விளக்கப்பட்டுள்ளபடி, பெரும்பாலான மறைகுறியீட்டுநாணயங்களின் அழிமாற்றத்தன்மை நிச்சயமற்றது, அதேநேரம் Epic Cash-யின் தனிமறைபு கட்டமைப்பு அதே அச்சுறுத்தல்களுக்கு ஆளாகாதவாறு உறுதி செய்கிறது.

Bitcoin-ஐ போன்ற பெரும்பாலான மறைகுறியீடுநாணயங்கள், அவை இயங்கும் வெளிப்படையான பிளாக்செயின்களின் தன்மையால், அவைகளை வைத்திருந்த ஒவ்வொரு வாலட்களின் மூலம் சரியாக கண்டறிய இயலும். தனியார் மூன்றாம் தரப்பினரும் அரசாங்கங்களும் Bitcoin பிளாக்செயினை அதிநவீன வழிமுறைகளுடன் நாணயங்களின் முந்தய செயல்பாட்டை விரைவாக அடையாளம் காண பெரிய அளவில் கண்காணிக்கின்றன. இது இயற்கையாகவே ஒருநாள் கறைபடிந்த நாணயங்கள் பரிவர்த்தனைகளில் இருந்து தடைசெய்யப்படக்கூடும் என்ற கவலைக் கு வழிவகுக்கிறது, இதனால் அவைகளில் நம்பிக்கை வைத்திருப்பவர்கள் நஷ்டத்தில் உள்ளாவர்.

மார்ச் 19, 2018 அன்று, U.S. வெளிநாட்டு சொத்து கட்டுப்பாட்டு அலுவலகம் (OFAC), இலக்கமுறை நாணய முகவரிகளை விசேஷமாக நியமிக்கப்பட்ட தேசியவாதிகள் (SDN-கள்) பட்டியலில் சேர்ப்பது குறித்து பரிசீலிப்பதாக அறிவித்தது, அவைகளோடு U.S. நபர்களோ அல்லது வணிகங்களோ பரிவர்த்தனை செய்ய தடை விதிக்கப்பட்டுள்ளன. இதிலும் சிக்கலானது, தற்போது கறைபடிந்த நாணயங்களை கொண்டுள்ள முகவரிகளை SDN பட்டியலில் சேர்ப்பதை OFAC நிராகரிக்கவில்லை, இது கறைபடிந்த மறைகுறியீட்டுநாணயங்களின் அப்பாவி உரிமையாளர்களை, கறைபடிந்த நாணயங்களுடனான தொடர்பு காரணமாக, குற்றவியல் தடுப்புப்பட்டியலில் அவர்களை சேர்க்கும். இது நியூயார்க் பல்கலைக்கழக சட்டப் பேராசிரியர், Andrew Hinkes-ஐ, "அழிமாற்றத்தன்மைக்கு பிரியாவிடை வாழ்த்துக்கள்" என்றும், பொதுமக்கள் "புதிதாகத் தயாரிக்கப்பட்ட நாணயங்களுக்கு அல்லது கண்டறிந்த சுத்தமான நாணயங்களுக்கு மிகைமதிப்பு.." எதிர்பார்க்க வேண்டும் என்றும் நகைக்க வழிவகுத்தது[8].

இந்த முன்னேற்றங்களை மனதில் கொண்டு, மறைகுறியீட்டு சந்தையில் ஒரு எழுச்சியையும், நன்கு-நிறுவப்பட்ட பல மறைகுறியீட்டுநாணயங்களின் துன்பங்களையும், அழிவையும் கற்பனை செய்வது கடினம் அல்ல. இருப்பினும், இந்த அறிக்கையில் முன்னர் விவரிக்கப்பட்டுள்ள வலுவான தனிமறைபு அம்சங்கள் காரணமாக இந்த சிக்கலை முற்றிலுமாக தவிர்க்கும் சில மறைகுறியீட்டுநாணயங்களில் Epic-யும் ஒன்றாகும். அடையாளம் மற்றும் உரிமையுடனான தொடர்பையும், பரிவர்த்தனை செய்யும் தரப்பினர்களுக்கு இடையிலான உறவையும் அகற்றுவதன் மூலம், Epic-ஐ ஒருபோதும் ஒரு நபருடனோ அல்லது ஒரு செயலுடனோ இணைக்க முடியாது. அதுபோல, Epic-யின் மதிப்பு அதன் பயனர்களிடமிருந்து சுதந்திரமானது மேலும் குற்றவியல், நிதி மற்றும் அரசியல் அரங்கங்களில் தீங்கிழைப்போரால் எளிதில் கையாள முடியாத உயர் தணிமறைபு மற்றும் பாதுகாப்பை வழங்குகிறது.

> "**. . . கறைபடிந்த நாணயங்கள் அழிவுகரமானவை. நீங்கள் அழிமாற்றத்தன்மை மற்றும் தனிமறைபு ஆகியவற்றை உடைத்தால், நீங்கள் நாணயத்தை உடைக்கிறீர்கள்.**"
>
> **ANDREAS ANTONOPOULOS**

[6] Njui, John P, ***Charlie Lee: Litecoin (LTC) To Soon Have Confidential Transactions for Fungibility***, 29 January, 2019, https://ethereumworldnews.com/charlie-lee-litecoin-ltc-to-soon-have-confidential-transactions-for-fungibility/

[7] Carl T, ***Andreas Antonopoulos Says If Fungibility Is Not Fixed Bitcoin Could Be Attacked,*** 9 April, 2019, https://bitcoinexchangeguide.com/andreas-antonopoulos-says-if-fungibility-is-not-fixed-bitcoin-could-be-attacked/

[8] Hinkes, Andrew, Ciccolo, Joe, ***OFAC's Crypto Blacklist Could Change Crypto***, 24 March, 2018, https://www.coindesk.com/goodbye-fungibility-ofacs-bitcoin-blacklist-remake-crypto

IV. அளவிடுதல்

Epic Cash என்பது ஒரு MimbleWimble பிளாக்செயின் செயலாக்கம் ஆகும், இடத்தை சரியாக பயன்படுத்தும் வடிவமைப்பின் விளைவாக, இது தேவையற்ற பரிவர்த்தனை தரவைக் களைந்து அளவிடுதலில் முன்னேற்றத்தை அளிக்கிறது. இதற்கு காரணமான Cut-Through செயல்பாடு, Bitcoin உள்ளிட்ட பெரும்பாலான மறைகுறியீட்டுநாணயங்களைப் போலல்லாமல், காலப்போக்கில் பிளாக்செயின் அதிக இடம் மிக்கவையாக வளர்கிறது என்பதையும், நினைவகம் மற்றும் கணினி ஆற்றலில் குறைந்த முதலீடுகளுடன் புதிய முனைகளை உருவாக்க முடியும் என்பதையும் உறுதிப்படுத்துகிறது. இடம்மிக்கவையாக இருப்பதால், இது பரவலாக கலைக்கப்பட்ட பிணையத்தை திறன்படுத்துவதுடன் பரவலாக்கலை வளர்க்கிறது. ஒவ்வொரு Bitcoin முனையும் முழுச் சங்கிலித்தொடரையும் சேமிக்க வேண்டும், ஆனால் Epic Cash முனைகள் தொகுதியின் ஒரு சிறிய துணையின் அடிப்படையில் பிணைய பாதுகாப்புக்கு பங்களிக்க முடியும்.

பெரும்பாலான மறைகுறியீட்டுநாணயங்களுக்கு அவற்றின் பிளாக்செயினில் அனைத்து பரிவர்த்தனை தரவையும் காலவரையின்றி சேமிக்க வேண்டும். Bitcoin-னின் சங்கிலித்தொடர் தற்போது ஒவ்வொரு நாளும் 0.1353 GB நினைவகத்தைப் அதிகரிக்கிறது, அதே நேரத்தில் Ethereum-த்தின் சங்கிலித்தொடர் ஒரு நாளுக்கு 0.2719 GB வேகத்தில் அதிகரிக்கிறது. Bitcoin-னின் சங்கிலித்தொடர் அதன் தற்போதைய விகிதத்தில் தொடர்ந்து வளர்ந்து கொண்டே இருந்தால், 2140 ஆம் ஆண்டில் அதன் கடைசி வெகுமதி தொகுதியை மைன் செய்யும் நேரத்தில் அது தோராயமாக 6 TB அளவை எட்டும். அந்த தேதிக்குள் Ethereum 10 TB-ஐ தாண்டும்[9]. MimbleWimble இல்லாத பெரும்பாலான மறைகுறியீட்டுநாணயங்களில், பரிவர்த்தனைகள் உலகெங்கிலும் உள்ள முனைகளால் சரிபார்க்கப்பட வேண்டும். தரவு அதிகரிக்கும் போது, ஒவ்வொரு முனையிலுமான சுமையும் அதிகரிக்கும். 200 GB (தற்போதைய Bitcoin சங்கிலித்தொடரின் தோராயமான அளவு), தரவைகளை ஒத்திசைக்க நிலையான பிணையம் மற்றும் படிக்கவும் எழுதவும் திறனுள்ள அதிவேக வட்டு தேவைப்படுகிறது.

இதன் விளைவாக, மைனிங் பெருமளவில் விலையுயர்ந்த கணினி வளங்களைக்கொண்ட பெரிய பூல்களின் மத்தியில் மையப்படுத்தப்பட்டதாக மாறியுள்ளது. **Bitcoin-னின் முழு பிளாக்செயின் வரலாற்றையும் Epic Cash பிளாக்செயினில் சேமிக்கப்பட வேண்டும் என்றால், அது கிட்டத்தட்ட 90% குறைவான இடத்திற்குள் பொருந்தும். சிறியது விரைவானது,** ஏனெனில் ஒவ்வொரு பரிமாற்றத்தை கடத்தவும் பாதுகாக்கவும் குறைந்த நேரம் தேவைப்படுகிறது.

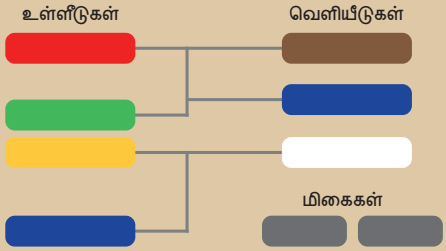
MimbleWimble இந்த தேக்கத்தின் குழப்பத்தை, 'Cut-Through' என குறிப்பிடப்படும் ஒரு புதுமையான தொகுதி கத்தரித்தல் மூலம் தீர்க்கிறது. Cut-Through எவ்வாறு செயல்படுகிறது என்பதைப் புரிந்துகொள்வதற்கு, ஒரு MimbleWimble பிளாக்செயினுக்குள் பரிவர்த்தனைகள் மற்றும் தொகுதிகள் எவ்வாறு உருவாக்கப்படுகின்றன என்பதை முதலில் பார்ப்பது நல்லது.

உள்ளீடுகள்:
பழைய வெளியீடுகள் பற்றிய குறிப்புகள்;

வெளியீடுகள்:
ரகசிய பரிவர்த்தனை வெளியீடுகள் மற்றும் வரம்புச்சான்றுகள்;

மிகைகள்:
வெளியீடுகள் மற்றும் உள்ளீடுகளுக்கு இடையேயான வேறுபாடு, மற்றும் ஒப்பங்கள் (அங்கீகாரத்திற்கும் பணவீக்கமற்றதை நிரூபிக்கவும்);

படம் 2:
MimbleWimble பரிவர்த்தனை பாகங்கள்.



[9] Li, Crypto, *Blockchain's Big Data Problem,* 27 January, 2019, https://www.longhash.com/news/blockchains-big-data-problem

அனைத்து Epic Cash பிளாக்குகளில் உள்ளவை:

பரிவர்த்தனை உள்ளீடுகளின் Merkle Trees;

பரிவர்த்தனை வெளியீடுகள் மற்றும் வரம்பு சான்றுகளின் Merkle Trees;

அதிகப்படியான மதிப்புகள் மற்றும் கையொப்பங்களின் பட்டியல்.

Andrew Poelstra-வின் விளக்கக்காட்சிகளிலிருந்து[10] எடுக்கப்பட்ட படங்கள் 2 மற்றும் 3-இல், புதிதாக மைன் செய்யப்பட்ட Epic வெள்ளை உள்ளீட்டு கலங்களாகக் காணலாம். ஒரே மாதிரியான வண்ணமிடப்பட்ட கலங்கள் செலவளிக்கப்பட்ட உள்ளீடுகளுடன் தொடர்புடைய வெளியீடுகளைக் குறிக்கின்றன. Cut-Through செயல்பாட்டின் மூலம், உள்ளீடுகளும் அதனுடன் பொருந்தக்கூடிய வெளியீடுகளும் பிளாக்கினுள் இடத்தை விடுவிக்க அகற்றாடுகின்றன, இது பிளாக்செயினில் சேமிக்க வேண்டிய தரவின் அளவைக் குறைக்கிறது. பரிவர்த்தனைகள் பேரேட்டிலிருந்து விலக்கப்பட்டாலும், மீதமுள்ள அதிகப்படியான கரு (வெறும் 100 பைட்டுகள்) பரிவர்த்தனைகள் நடந்ததாக நிரந்தரமாக ஆவணப்படுத்துகின்றன.

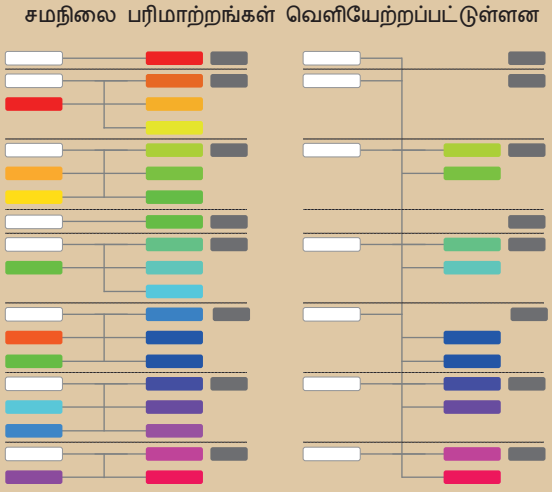
தொகுதிகள் தொடர்ந்து உருவாக்கப்படுவதால், MimbleWimble தொகுதிகள் முழுவதும் Cut-Through-வை பயன்படுத்துகிறது, இதனால் நீண்ட காலத்திற்கு மேல் தொகுதிகளின் தலைப்புகள் (தோராயமாக 250 பைட்டுகள்), செலவிடப்படாத பரிவர்த்தனைகள் மற்றும் பரிவர்த்தனை கருக்கள் (தோராயமாக 100 பைட்டுகள்) மட்டும் மிஞ்சும். இரண்டாவதாக தொடங்கப்படும் MimbleWimble செயல்படுத்தலான Grin, Bitcoin சங்கிலித்தொடரைப் போன்ற எண்ணிக்கையிலான பரிவர்த்தனைகளைக் கொண்ட ஒரு MimbleWimble சங்கிலித்தொடர் Bitcoin-னின் சங்கிலித்தொடரின் அளவில் கிட்டத்தட்ட 10% ஆக இருக்கும் என்பதைக் காட்டியது[11]. மேலும், ஒரு முனையின் அளவு "Bitcoin அளவிலான சங்கிலித்தொடருக்கு ஒரு சில GB-யின் அளவில் இருக்கும், அதை சில நூறு MB-களாக மேம்படுத்த சாத்தியமுள்ளது.[12]"

இது Bitcoin-க்கு முற்றிலும் மாறுபட்டதாக உள்ளது, அங்கு முழு பிளாக்செயினும் ஒவ்வொரு முனையிலும் சேமிக்கப்பட வேண்டும். காலப்போக்கில், Epic Cash பிளாக்செயினின் பரப்பு செயல்திறன் Bitcoin பிளாக்செயினுடன் ஒப்பிடும்போது வளரும் போது, அதேபோல் Epic Cash பிணையத்தில் முனைகளின் பங்கேற்புடன் தொடர்புடைய செலவு செயல்திறன்களும் அதிகரிக்கும். பங்கேற்பதற்கான குறைந்த தடைகள் பிணைய வடிவமைப்பின் முனை அடுக்கில் முக்கியமான மீள்திறனை உறுதிப்படுத்த உதவுகின்றன.

MimbleWimble-ஐ அமல்படுத்துவதுடன் சங்கிலித்தொடரை Cut-Through செயல்முறையால் கத்தரிப்பதன் மூலம் Epic Cash பிளாக்செயின் மறைகுறியீட்டுநாணயங்களின் சமூகத்தால் பெரும்பாலும் கவனிக்கக்கூடிய வகையிலான அளவிடக்கூடிய தன்மையை வழங்குகிறது. இது Bitcoin மற்றும் ஒத்த எண்ணம் கொண்ட திட்டங்களின் சாரத்தைப் பிடிக்கும் ஒன்றாகும்: பரவலாக்கம். ஒரு நாணயத்தை வினாடிக்கு எத்தனை பரிவர்த்தனைகள் செயலாக்க முடியும் என்பதைக்காட்டிலும், ஒரு பரந்த மற்றும் மாறுபட்ட பிணையத்தால் அதைத் தக்கவைக்க முடியாவிட்டால் என்ன நல்லது? நினைவக தேவைகள் சரிபார்ப்பின் இறுதியில் வலுவான மைனிங் நிறுவனங்களை ஈர்பதாக இருந்தால், ஒரு பரவலாக்கப்பட்ட சுற்றுச்சூழல் அமைப்பை உருவாக்குவதற்கான மறைகுறியீட்டுநாணய சமூகத்தின் அனைத்து முயற்சிகளும் தவிர்க்கப்படுகின்றன. கூடுதல் செயல்திறனை வழங்க, Epic Cash மேம்பாட்டு காலவரைபடத்தில் ஒரு குறுகிய கால நோக்கமாக மின்னல்-பாணியிலான அடுக்கு 2 செயல்படுத்த திட்டமிடப்பட்டுள்ளது.

படம் 3:

Cut-Through-வுக்கு முன்னும் பின்னுமான MimbleWimble பரிவர்த்தனைகள்.



[10] SF Bitcoin Developers, *MimbleWimble with Andrew Poelstra,* 24 November, 2016, https://www.youtube.com/watch?v=aHTRlbCaUyM&t=940s

[11] Grin Forum, *Grin Blockchain Size,* December, 2018, https://www.grin-forum.org/t/grin-blockchain-size/1334

[12] GandalfThePink, *Introduction to Mimblewimble and Grin,* 28 March, 2019, https://github.com/mimblewimble/grin/blob/master/doc/intro.md

V. பணக்கொள்கை

Epic Cash மற்றும் Bitcoin ஆகியவற்றின் பணக்கொள்கை மிகவும் ஒத்திருக்கிறது. Epic Cash-ன் சுழற்சியிலுள்ள வழங்கீடு முதலில் விரைவில் விரிவடைந்து பின்னர் BItcoin 2028-இன் சுழற்சி வழங்கீடுடன் ஒத்திசைகிறது. இது அதிகரித்து அதன்பின் குறைந்துவரும் விகிதத்தில் 2140 இல் அதிகபட்சமாக 21 மில்லியன் Epic-ஐ எட்டும். Epic Cash அதன் உமிழ்வு ஆயுள்சுழற்சியின் காரணமாக ஒரு பாதுகாப்பான சேமிப்பாக நீண்டகால மதிப்பைக் கொண்டுள்ளது மேலும் நிலையான அதிகபட்ச வழங்கீடுடன் உச்சமடைகிறது. Epic Cash பணக்கொள்கை பின்வரும் நான்கு அம்சங்களால் வகைப்படுத்தப்படுகிறது:

- அதன் ஆயுட்காலத்தின் முதல் ஒன்பது ஆண்டுகளில் விரைவான உமிழ்வு, அப்போது 20,343,750 Epic (மொத்த வழங்கீட்டில் 96.875%) மைன் செய்யப்பட வேண்டும். இந்த அறிக்கையின் உமிழ்வு அட்டவணை பிரிவில் சரியான உமிழ்வு விகிதங்கள் கோடிட்டுக் காட்டப்பட்டுள்ளன;
- மே 24, 2028 இல் Epic Singularity-யின் போது Epic-யின் சுழற்சிலுள்ள வழங்கீடு மற்றும் உமிழ்வு வீதம் பிட்காயினுடன் ஒத்திசைக்கப்படுகிறது. Singularity-யை தொடர்ந்து, உமிழ்வு வீதம் அதிகரிக்கும் விகிதத்தில் குறைகிறது, அதே நேரத்தில் சுழற்சியிலுள்ள வழங்கீடு குறைந்துவரும் விகிதத்தில் வளர்கிறது;
- அதிகபட்ச வழங்கீடான 21 மில்லியன் Epic-கள் 2140 ஆம் ஆண்டில் அடையும், ஏறக்குறைய Bitcoin அதன் அதிகபட்ச வழங்கீடான 21 மில்லியன் அலகுகளை அடையும் நேரத்தில்;
- Epic-இல் 8 தசம வகுத்தல் அமைப்பு உள்ளது, அதாவது: 1 Epic 100,000,000 freeman-னுக்கு சமம் (1 Bitcoin 100,000,000 satoshi-க்கு சமமாவது போல).

Epic Cash பணக்கொள்கை பின்வரும் காரணங்களுக்காக Bitcoin-ஐ மாதிரியாகக் கொண்டு வடிவமைக்கப்பட்டுள்ளது:

- Bitcoin-னின் பொருளாதார அடிப்படைகளுடனான ஒப்பந்தம், அதாவது பற்றாக்குறையும் சுழற்சியிலுள்ள வழங்கீட்டை கணிக்கக்கூடிய தன்மையும் அதன் வலுவான மதிப்பு பண்புகளை அடிக்கோடிடுகிறது;
- Bitcoin-னின் மாதிரி மற்றும் அதன் தொடக்கத்திலிருந்து கடந்த பத்து ஆண்டுகளில் அதன் நிரூபிக்கப்பட்ட தட பதிவு ஆகியவற்றை பொதுமக்கள் ஏற்கனவே அறிந்திருக்கிறார்கள். Bitcoin-னின் சுழற்சியிலுள்ள வழங்கீடுடன் தோராயமாக ஒத்திசைப்பதன் மூலமும், Bitcoin-னின் அதிகபட்ச வழங்கீடு மற்றும் வகுக்கும் கட்டமைப்பைப் பிரதிபலிப்பதன் மூலமும், Epic வெகுஜன பயன்பாட்டிற்கு குறைந்த எதிர்ப்பின் பாதையை எடுக்கிறது.

VI. உமிழ்வு அட்டவணை

Epic Cash-இல் மொத்தம் 33 மைனிங் காலங்கள் உள்ளன, ஒவ்வொன்றும் அவற்றின் முந்தைய காலத்துடன் ஒப்பிடும்போது தொகுதி வெகுமதிகளின் குறைவால் வைரயறுக்கப்படுகின்றன. Epic தொகுதி # 1 மைன் செய்யப்பட்ட தேதி, Epic Genesis, ஆகஸ்ட் 2019 அன்று நைடெபறுகிறது. தொகுதிகள் நிமிடத்திற்கு ஒரு முறை மைன் செய்யப்படுகின்றன. முதல் ஐந்து காலங்கள் Epic அதிகபட்ச வழங்கீட்டில் கிட்டத்தட்ட 97% உருவாக்குகின்றன, இது சுமார் ஒன்பது ஆண்டுகளில் 20 வருட Bitcoin உமிழ்வுகளுடன் பொருந்தும். Bitcoin-னின் கண்கவர் உயர்வைத் தவறவிட்டவர்களுக்கு இது 'கடிகாரத்தைத் திருப்புவதற்கான" வாய்ப்பாக கருதலாம்.

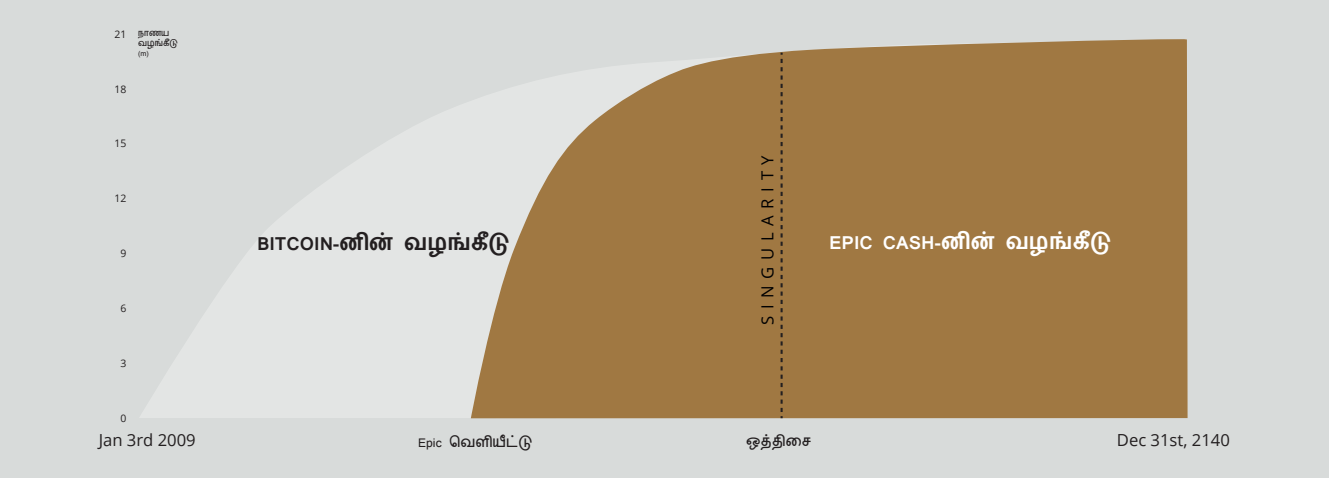
அட்டவணை 1 இல் உள்ள உமிழ்வு அட்டவணை, முதல் ஏழு மைனிங் காலங்களின் தொடக்க மற்றும் இறுதி தேதிகள், அவற்றுடன் தொடர்புடைய தொகுதி வெகுமதிகள், மற்றும் ஒவ்வொரு காலத்திற்குமான சுழற்சியிலுள்ள வழங்கீடு ஆகியவற்றைக் கோடிட்டுக் காட்டுகிறது. 8 முதல் 33 வரையிலான காலங்கள் சுருக்கத்திற்காக அட்டவணையில் சேர்க்கப்படவில்லை. அந்த காலங்களுக்கு, Bitcoin-ஐ போல ஒவ்வொரு அடுத்தடுத்த காலத்திற்குமான தொகுதி வெகுமதி முந்தைய காலத்தின் வெகுமதி அளவுக்கு பாதி என்பதைப் புரிந்துகொள்வது போதுமானது. ஒவ்வொரு காலகட்டத்திலும் வெளிப்படும் Epic-ன் அளவு 4 ஆண்டு காலத்திற்குண்டன (தோராயமாக 1460 நாட்கள்) தொகுதி வெகுமதிகளின் தொகையாகும்.

Epic Singularity-யில் (2028), Epic சுழற்சியிலுள்ள வழங்கீடு Bitcoin-னின் சுழற்சியிலுள்ள வழங்கீட்டின் எண்ணிக்கையை அடைகிறது, அந்த சமயத்தில் Epic Cash Bitcoin-னின் தொகுதி வெகுமதி மற்றும் halving முறையை ஏற்றுக்கொள்கிறது, இது தொகுதி வெகுமதிகளை ஒவ்வொரு நான்கு வருடங்களுக்கும் பாதியாக குறைக்கிறது. ஒரே விதிவிலக்கு என்னவென்றால், ஒவ்வொரு பத்து நிமிடங்களுக்கும் ஒரு தொகுதி என்ற Bitcoin-னின் வீதத்திற்கு எதிராக, ஒவ்வொரு நிமிட வீதத்தில் Epic தொகுதிகள் தொடர்ந்து மைன் செய்யப்படுகின்றன. இதைச் செய்வதன் மூலம், Epic-யின் சுழற்சியிலுள்ள வழங்கீடு Bitcoin-னின் சுழற்சியிலுள்ள வழங்கீடுடன் தோராயமான சமநிலையைப் பராமரிக்கிறது.

அட்டவணை 1: முதல் ஏழு மைனிங் காலங்களுக்கான உமிழ்வு அட்டவணை. தேதிகள் நெருங்கிய தோராயங்கள்.

காலம்	1	2	3	4	5	SINGULARITY	6	7
தொகுதி வெகுமதி	16	8	4	2	1		0.15625	0.078125
தொடக்க தேதி	Aug 1, 2019	Jun 29, 2020	Oct 11, 2021	Jun 3, 2023	Aug 10, 2025		May 24, 2028	May 22, 2032
இறுதி தேதி	Jun 29, 2020	Oct 11, 2021	Jun 3, 2023	Aug 10, 2025	May 24, 2028		May 22, 2032	May 20, 2036
நீளம் (நாட்களில்)	334	470	601	800	1019		1460	1460
தொடக்க வழங்கீடு	0	7,695,360	13,109,760	16,571,520	18,875,520		20,342,880	20,671,380
இறுதி வழங்கீடு	7,695,360	13,109,760	16,571,520	18,875,520	20,342,880		20,671,380	20,835,630
அதிகபட்ச வழங்கீட்டின் %	36.6%	62.4%	78.9%	89.9%	96.9%		98.4%	99.2%

படம் 4: Epic மற்றும் Bitcoin -னின் உமிழ்வு அட்டவணைகள்.



VII. மைனிங்

Epic Cash பிளாக்செயின் பல்வகையான கணக்கீட்டு வன்பொருள்களை வரவேற்பதன் மூலம் பரவலாக்கலைத் தொடர்கிறது. Epic மைனிங் ஆரம்பத்தில் CPU, GPU மற்றும் ASIC களுக்கு, RandomX, ProgPow, and CuckATOO31+ ஆகிய மூன்று ஹாஷிங் தீர்வுநெறிகளைப் பயன்படுத்தி கிடைக்கப்பெறும். சங்கிலித்தொடரின் ஒருமைப்பாட்டை சமரசம் செய்யாமல் தீர்வுநெறிகளை எளிமையாக மாற்றலாம்.

1 RandomX மற்றும் CPU-க்கள்

RandomX என்பது பொதுப்பயனுக்கான CPU-க்களுக்கு உகந்த ஒரு PoW தீர்வுநெறி ஆகும். பின்வரும் குறிக்கோள்களை அடைய இது பல Memory-hard நுட்பங்களுடன் சீரற்ற நிரல் செயற்பாங்குகளைப் பயன்படுத்துகிறது:

- ஒற்றை-சில்லு ASIC-களின் வளர்ச்சியைத் தடுக்கும்;
- பொதுபயனுக்கான CPU-க்களில் சிறப்பு வன்பொருளின் செயல்திறன் மேன்மையைக் குறைக்கவும்.

Epic-யை மைனிங் செய்யும் CPU-க்களுக்கு மைனிங் புரி ஒன்றுக்கு 2 GB RAM, 16 KB L1 இடைமாற்று, 256 KB L2 இடைமாற்று மற்றும் 2 MB L3 இடைமாற்று ஒதுக்கீடு தேவைப்படுகிறது[13]. Windows 10 சாதனங்களுக்கு 8 GB அல்லது அதற்கு மேற்பட்ட RAM தேவைப்படும். வருங்கலத்தில் ஒரு நாள் அலைபேசிகள் மைனிங் முனைகளாக செயல்படக்கூடும் என்பது நினைக்கமுடியாத ஒன்றாக இருக்காது. Epic Cash மைனிங் பிணையத்தில் CPU-வை ஆரம்பகாலத்தில் ஒருங்கிணைத்தால் சாதாரண கணினி வழிமுறைகளைக் கொண்ட பலருக்கும் Epic Cash பிணையத்தை பாதுகாக்க உதவுவதன் மூலம் பிளாக் வெகுமதிகளைப் பெறுவதற்கான ஒரு சிறந்த வாய்ப்பாக அமையும்.

2 ProgPow மற்றும் GPU-க்கள்

Programmatic Proof-of-work (ProgPow) என்பது ஒரு தீர்வுநெறி ஆகும், இது நினைவக அலைக்கற்றையையும் சீரற்ற கணித வரிசைகளின் முக்கிய கணக்கீடுகளையும் பொறுத்தது, இது ஒரு GPU-வின் கணினி அம்சங்களில் பலவற்றைப் பயன்படுத்தி, அதன் மூலம் வன்பொருளின் மொத்த ஆற்றல் செலவை திறம்படச்செய்கிறது. Progpow குறிப்பாக பொருட்களின் GPU-க்களை முழுமையாகப் பயன்பெற வடிவமைக்கப்பட்டுள்ளதால், சிறப்பு வன்பொருள் மூலம் அதிக செயல்திறனை கணிசமாக அடைவது கடினமானதும் விலையுயர்ந்ததும் ஆகும். எனவே, ProgPow தீர்வுநெறி, Bitcoin-னின் SHA-256 போல பெரும்பாலான பல PoW தீர்வுநெறிகளில் காண்பதுபோன்று, பெரிய ASIC பூல்களின் சலுகைகளை GPU-க்களை விஞ்சுவதற்காக குறைக்கிறது. GPU-க்கள், CPU-க்களைப் போல அதிகம் இல்லை என்றாலும், பொதுவாக கிடைக்கின்றன. தொழிற்நுட்ப வளர்ச்சியால் இயக்கப்படும் Nvidia மற்றும் AMD போன்ற வலுநிலைகளால், GPU-க்களால் CPU-க்களை விட, ஒரு அலகு அடிப்படையில், பல மடங்கு மைனிங் தீர்வுகளை இணையாக செயலாக்க முடியும். அட்டவணை 2 இல் சுட்டிக்காட்டப்பட்டுள்ளபடி, எங்கும் நிறைந்திருப்பதாலும் உயர் செயலாக்க சக்தியினை கொண்டதாலும், GPU-க்கள் ஆரம்பகால மைனிங் நடவடிக்கைகளின் பெரும்பகுதிக்கு முதுகெலும்பாக விழுங்கும்.

3 CuckATOO+31 மற்றும் ASIC-கள்

CuckATOO31+ என்பது டச்சு கணினி விஞ்ஞானி, John Tromp உருவாக்கிய Cuckoo Cycle தீர்வுநெறியின் ASIC நட்பு வரிசைமாற்றமாகும். ASIC எதிர்ப்பு CuckARoo29-விற்கு ஒப்புமையுடையது, CuckATOO31+ சீரற்ற இருதரப்பு வரைபடங்களை உருவாக்குவதுடன் மைனிங் செய்பவர்களுக்கு அந்த வரைபடத்தின் முகடுகளைக் கடந்து செல்லும் கொடுக்கப்பட்டுள்ள 'N' நீள சுழற்சியைக் கண்டுபிடிக்கும் பணியை வழங்குகிறது.

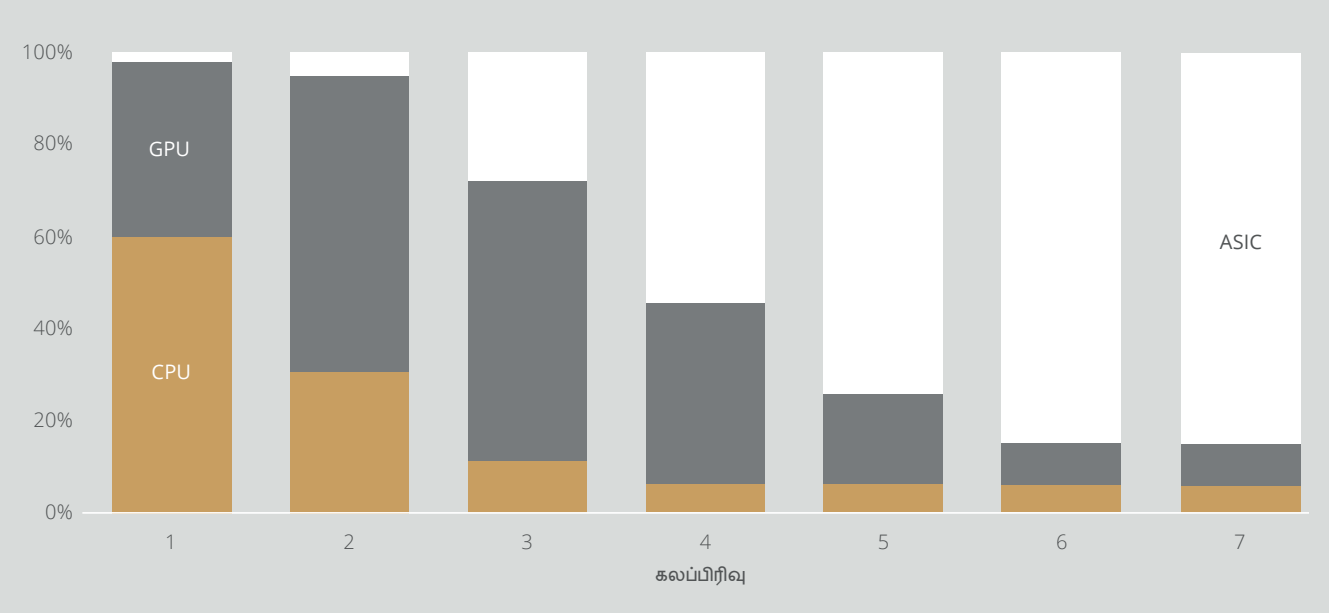
[13] Tevador, *RandomX*, 28 மார்ச், 2019, https://github.com/tevador/RandomX

இது நினைவகம் சார்ந்த பணியாகும், அதாவது தீர்வு நேரம் மூல செயலி அல்லது GPU-வின் வேகத்தை விட நினைவக அலைகற்றையால் கட்டுப்படுத்தப்படும். இதன் விளைவாக, Cuckoo Cycle தீர்வுநெறிகள் குறைந்த வெப்பத்தை உருவாக்குவதுடன் பாரம்பரிய PoW தீர்வுநெறிகளை விட கணிசமாக குறைந்த ஆற்றலை பயன்படுத்துகின்றன. ASIC நட்பு CuckAToo31+ ஆனது SRAM-ன் நூற்றுக்கணக்கான MB-களை பயன்படுத்துவதன் மூலம் GPU-க்களை விட செயல்திறனை மேம்படுத்த அனுமதிக்கிறது, அதே நேரத்தில் நினைவகம் I/O மூலம் கட்டுப்படுத்தப்படுகிறது[14]. இறுதியில், ASIC-கள் மூன்று மைனிங் முறைகளில் மிகப்பெரிய சாத்தியமான பொருளாதாரங்களை வழங்குகின்றன. எவ்வாறாயினும், அனைவரையும் உள்ளடக்கும் ஆர்வத்தில், ஆரம்பத்தில் CPU-க்கள் மற்றும் GPU-க்களுடன் ஒப்பிடும்போது மைனிங் வெகுமதிகளில் சிறிய பகுதி அவைகளுக்கு ஒதுக்கப்படிருந்தாலும், இறுதியில் ASIC-கள் பெரும்பகுதியான மைனிங் செய்யப்பட்ட தொகுதி வெகுமதிகளை எடுத்துக்கொள்கின்றன என்பது, CuckAToo31+-க்கான சாதன உற்பத்தியாளர்களிடையே போட்டி சுற்றுச்சூழல் அமையும் என்ற அனுமானத்தில்.

அட்டவணை 2: மைனிங் வெகுமதி ஒதுக்கீடு. திருத்தத்திற்கு உட்பட்டது. அதிகபட்ச பரவலாக்கலை அடைவதற்கும், பிணையத்தின் நீண்டகால நலன்களுடன் ஒத்துப்போகவும் ஒதுக்கீடுகள் இயக்கப்படும்

காலப்பிரிவு	1	2	3	4	5	6	7
நாட்கள்	334	470	601	800	1019	1460	1460
CPU-க்கள்	60%	30%	10%	5%	5%	5%	5%
GPU-க்கள்	38%	65%	62%	40%	20%	10%	10%
ASIC-கள்	2%	5%	28%	55%	75%	85%	85%

படம் 5: அட்டவணை 2 இன்படி ஒவ்வொரு காலப்பிரிவிற்குமான மைனிங் வெகுமதி ஒதுக்கீடு. திருத்தத்திற்கு உட்பட்டது.



[14] Le Sceller, Quentin, *Grin ப்ரூப்-ஆப்-ஒர்க் பற்றி ஒரு அறிமுகம்*, 16 நவம்பர், 2018, https://blog.blockcypher.com/an-introduction-to-grin-proof-of-work-103aaa9f66ce

4 மைனிங் பங்களிப்புகள்

Epic Genesis (2019) தொடங்கி, Epic Singularity (2028) வரை, மைனிங் செயல்பாட்டின் போது, மைனிங் பங்களிப்பாக, EPIC பிளாக்செயின் அறக்கட்டளையை நோக்கி திருப்பி விடப்படும் Epic ஒதுக்கீடு உள்ளது.

EPIC பிளாக்செயின் அறக்கட்டளை தொழில்நுட்ப மேம்பாட்டிற்காகவும், Epic Cash திட்டத்தின் தொடக்க ஆண்டுகளில் விழிப்புணர்வு மற்றும் பயன்பாட்டை ஊக்குவிப்பதற்காகவும், சந்தைப்படுத்தல் நடவடிக்கைகளை உருவாக்கவும், நிதி தொழில்நுட்பத் துறையில் கூட்டாண்மையினை வளர்க்கவும் அர்ப்பணிக்கப்பட்டுள்ளது.

Singularity-க்கு பிறகு, EPIC அறக்கட்டளையின் பங்கு EPIC விநியோகிக்கப்பட்ட தன்னாட்சி கழகத்தால் (EDAC) ஏற்றுக்கொள்ளப்படும், இது ஒப்படைக்கப்படுவதற்கு முன்னர் அறக்கட்டளையால் உருவாக்கப்படும்.

EPIC பிளாக்செயின் அறக்கட்டளை மைனிங் வெகுமதிகளின் ஒரு பகுதியால் நிதியளிக்கப்படுகிறது, இது பின்வரும் ஆண்டு விகிதங்களின்படி தொகுதி வெகுமதிகளிலிருந்து கழிக்கப்படுகிறது:

அட்டவணை 3: மைனிங் வெகுமதிகளின் சதவீதமாக, அறக்கட்டளை மைனிங் பங்களிப்புகளின் ஆண்டு விகிதங்கள்.

ஆண்டு	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028
மைனிங் வெகுமதிகளின் %	8.88 %	7.77 %	6.66 %	5.55 %	4.44 %	3.33 %	2.22 %	1.11 %	1.11 %	0 %

VIII. முடிவுரை

பரவலாக்கப்பட்ட இலக்கமுறை தங்கமாக Bitcoin அங்கீகரிக்கப்பட்ட நிலைக்கு எதிரிணையாக Epic ஒரு பரிமாற்ற ஊடகமாக 'பரவலாக்கப்பட்ட இலக்கமுறை வெள்ளி'என அங்கீகரிக்கப்படுவதை நோக்கமாகக் கொண்டுள்ளது. இழந்த அழிமாற்றத்தன்மையை அதிக ஆற்றல்-திறனுள்ள மற்றும் சுற்றுச்சூழல்-நட்புமிக்க வன்பொருளின் முதுகெலும்பில் மீண்டும் அறிமுகப்படுத்துவதன் மூலம், Epic Cash அதிகாரத்தின் சமநிலையை மீண்டும் தனிப்பட்ட பயனர்களுக்கு சாதகமாக சாய்த்து, சமீபத்திய மையப்படுத்தும் போக்குகளுக்கு முற்றிலும் மாறுபட்டதாக அமையும். Bitcoin பொருளாதாரம், விளையாட்டுக் கோட்பாடு மற்றும் நிரூபிக்கப்பட்ட PoW சூத்திரம் ஆகியவற்றின் கலவையை சமகால பிளாக்செயின் தொழில்நுட்பத்துடன் சேர்த்தால் நம்பகமான, மாறாத, பரவலாக்கப்பட்ட நாணயத்தை (Epic) உருவாக்கும், அது அளவிடக்கூடியதாகவும், அழிமாற்றத் தன்மையுடையதாகவும், பயனர்களின் தனிமறைபை பாதுகாக்கூடியதாகவும் அமையும். Epic Cash ஒரு திறந்த, பொது, எல்லையற்ற மற்றும் தணிக்கை-எதிர்ப்பு பிளாக்செயின் ஆகும். இது அதன் பயனர்களின் தனிமறைபையும் செல்வத்தையும் பாதுகாக்கிறது மேலும் மைனிங் வழியாக பிணையத்திற்கு ஆதரவாக தங்கள் வன்பொருளைப் பயன்படுத்துபவர்களுக்கு வெகுமதி அளிக்கிறது. ஒவ்வொரு Epic-கும் PoW மூலம் மைன் செய்யப்படுகிறது. வழங்கீடு பூஜ்ஜியத்தில் தொடங்குகிறது மேலும் பிணையம் நியாயமாக தொடங்கப்பட்டதாகக் கருதப்படுகிறது, செயல்படும் டெஸ்ட்நெட் தற்போது இயங்குகிறது.

Epic Cash முக்கிய உண்மைகள்:

- **மைனிங் ஆகஸ்ட் 2019 முதல் தொடங்குகிறது.**
- **Epic Cash பிளாக்செயின் MimbleWimble-ஐ அடிப்படையாகக் கொண்டது.**

  நெறிமுறையின் வைரயறுக்கும் அம்சங்கள்:

  1. **Cut-Through** - இடைவெளி திறனை மேம்படுத்துவதற்கும், பிணைய சரிபார்ப்பில் பரவலான பங்கேற்பை ஊக்குவிப்பதற்கும், பரவலகத்திற்கும், பிளாக்செயினிலிருந்து தேவையற்ற தகவல்களை நீக்குதல்;
  2. **CoinJoin** - Epic மறைகுறியீட்டுநாணயம் அழிமாற்றத்தன்மையை உறுதிப்படுத்த ஒரு பிளாக்கிற்குள் பரிவர்த்தனைகளை தொகுத்தல்;
  3. **Dandelion++ நெறிமுறை** - பின்னிப்பிணைந்த தடங்களில் தொடர்பு கொள்வதன் மூலம் பரிவர்த்தனைகளை பரப்புதல், முனைகளின் பரந்த பிணையத்தில் பரவுதல், பரிவர்த்தனைகளுக்கும் அவற்றின் தோற்றத்திற்கும் இடையிலான தொடர்புகளைத் துண்டித்தல்;
  4. **வாலட் முகவரிகள் இல்லை** - பரிவர்த்தனை செய்வதற்கு ஒற்றை-பயன்பாட்டு தனியார் விசை உருவாக்க ஒரு பெரிய Multisignature-ன் பயன்பாடு, வாலட் முகவரிகளின் தேவையை முற்றிலுமாக நீக்குகிறது.

- **Epic Cash-யின் நாணயக் கொள்கையானது** Epic-யின் சுழற்சியிலுள்ள வழங்கீடு ஏறக்குறைய ஒன்பது ஆண்டுகளில் Bitcoin-னின் சுழற்சியிலுள்ள வழங்கீடுடன் ஒத்திசைக்க வடிவமைக்கப்பட்டுள்ளது, மேலும் 2140 ஆம் ஆண்டில், அதிகபட்ச வழங்கீடான 21 மில்லியன் அலகுகளை எட்டும். இந்த குறைந்துவரும் பணவீக்கக் கொள்கை வெளிப்படைத்தன்மை, வழங்கீட்டின் முன்கணிப்பு, பற்றாக்குறை ஆகியவற்றை உறுதி செய்கிறது, இது நீண்ட கால சேமிப்பின் மதிப்பை பாதுகாத்து வளர்க்கிறது.

- **மைனிங்** திரளான பயன்பாட்டினையும் பிணையத்தின் செயல்திறனையும் எளிதாக்குவதற்காக, CPU-க்கள், GPU-க்கள் மற்றும் ASIC-களை அதன் தொடர்புடைய RandomX, ProgPow மற்றும் CuckATOO31+ தீர்வுநெறிகள் வழியாக இணைக்கும்.

IX. தொழில்நுட்ப விவரக்குறிப்புகள்

திட்டத்தின் பெயர்: Epic Cash

நாணயத்தின் பெயர்: Epic

தொகுதி நேரம்: 60 வினாடிகள்

தொகுதி அளவு: 1 MB

தொடக்க வழங்கீடு: 0

இறுதி வழங்கீடு: 21,000,000

முதல் தொகுதி: ஆகஸ்ட் 2019

கருத்திணக்கம்: RandomX (CPU-க்கள்), ProgPow (GPU-க்கள்) and CuckAToo31+ (ASIC-கள்)

இணைப்புகள்:

www.epic.tech

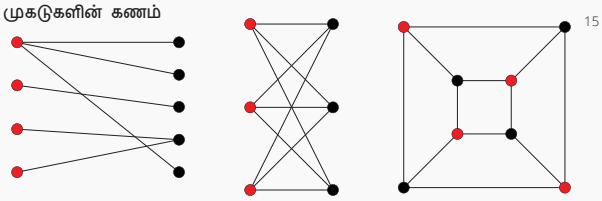
t.me/EpicCash – Telegram

t.me/EpicCashTamil

X. சொற்களஞ்சியம்

ASIC
குறிப்பிட்ட பயன்பாட்டிற்கான ஒருங்கிணைந்த சுற்றுகள்; ஒற்றை நோக்கத்திற்காக வடிவமைக்கப்பட்ட சில்லுகள்

இருதரப்பு வரைபடம்
ஒரே கணத்திற்குள் இரண்டு வைரபட முகடுகள் அடுத்தடுத்து இல்லாத வைகயில், இரண்டு வெட்டாக்கணங்களாக சிதைந்த வைரபட முகடுகளின் கணம்


[15]

மறைக்கும் காரணிகள்
குறியாக்கத்தை எளிதாக்க இலக் கமுறை செய்தியில் அறிமுகப்படுத்தப்படும் ஒரு சீரற்ற உறுப்பு; ஒரு குறிப்பிட்ட பரிவர்த்தனையில் உள்ளீடுகள் மற்றும் வெளியீடுகளையும் பரிவர்த்தனை செய்யும் நபர்களின் பொது மற்றும் தனியார் விசைகளையும் குறியாக்கம் செய்யும் இரு தரப்பினருக்கும் இடேய பகிரப்பட்ட ரகசியம்[16].

தொகுதி வெகுமதிகள்
ஒரு புதிய தொகுதிக்குள் பரிவர்த்தனைகளை சரிபார்க்க நிகழ்த்தப்பட்ட கணக்கீடுகளுக்கான வெகுமதிகளாக பிணையத்தால் விநியோகிக்கப்பட்ட புதிய Epic.

இடைமாற்று
தரவைச் சேமிக்கும் ஒரு வன்பொருள் அல்லது மென்பொருள் கூறு, இதனால் அந்தத் தரவிற்கான எதிர்கால கோரிக்கைகள் விரைவாக வழங்கப்படும்.

சுழற்சியிலுள்ள வழங்கீடு
ஒரு குறிப்பிட்ட நேரத்தில் இருக்கும் Epic-யின் அளவு.

CPU
மத்திய செயலாக்க பிரிவு: கணினியின் பிற வன்பொருள் மற்றும் மென்பொருளிலிருந்து பெரும்பாலான கட்டளைகளை விளக்கி செயல்படுத்துவதற்கான கணினி கூறு.

Cut-Through
ஒரு MimbleWimble பிளாக்செயின் செ யல்முறை, உள்ளீடுகளும் அதனுடன் பொருந்த க்கூடிய வெளியீடுகளும் தொகுதியில் இடத்தை விடுவிக்க அகற்றப்படுகின்றன, இது பிளாக்செயினில் சேமிக்க வேண்டிய தரவின் அளவைக் குறைக்கிறது.

பரவலாக்கம்
பிணையத்தின் செயல்பாடுகள் மற்றும் நிர்வாகத்தின் சிதறலின் நிலை.

உமிழ்வு
மைனிங் செய்பவர்கள் தொகு தி வெகும திகளாக சம்பா தித்த புதிய E pic-ஐ உருவாக்கு தல். பிளாக்செயினில் பரிவர்த்தனைகள் உறுதி செய்யப்படுவதால் ஒவ்வொரு 60 விநாடிகளிலும் Epic உருவாக்கப்படுகிறது.

Epic Singularity
Epic-யின் சுழற்சியிலுள்ள வழங்கீடு Bitcoin-னின் சுழற்சியிலுள்ள வழங்கீடுடன் ஒத்திசைகிறது (மே 2028).

மிகை (MimbleWimble)
வெளியீடுகள் ம ற்றும் உள்ளீடுகளுக்கு இடையேயான வேறுபா டு, மற்றும் கையொப்பங்கள் (அங்கீகாரத்திற்கும் பணவீக்கமற்றதை நிரூபிக்கவும்);

அழிமாற்றத்தன்மை
ஒரு பொருளின் ப ண்பு, இத ன் மூலம் தனிப் பட்ட அலகுகள், அடிப்படைய ில் ஒன்றுக்கொன்று மாறக்கூடியவை, மேலும் அதன் ஒவ்வொரு பகுதியும் மற்றொரு பகுதியிலிருந்து பிரித்தறிய முடியாதவை.

Genesis (நிகழ்வு)
முதல் Epic தொகுதியை மைனிங் செய்வது மற்றும் பிளாக்செயினின் அதிகாரப்பூர்வ ஆரம்பம்.

GPU
வரைகலை செயலாக்க அலகு: காட்சி செயல்பாடுகளுக்கு சிறப்புமிக்க ஒரு நிரல்படுத்தக்கூடிய ஏரண சில்லு (செயலி) கொண்ட ஒ ரு அ லகு. மறைகுறியீட்டுநாணயங்கள் மைனி ங் செய்வத ற்கு நுகர்வோர் GPU-க்கள் நன்கு பொருத்தமாக இருக்கும்.

Halving (Bitcoin-க்கு)
ஒவ்வொரு 4 வ ருடங்களுக்கு நிகழ்கிறது. ஒவ்வொ ரு halvi ng நிகழ்விற்கு பின்னரும் வழங்கீடு விகிதம் 50% குறைகிறது.

ஹாஷ்
ஹாஷிங் செயல்பாட்டைப் பயன்படுத்தி அடிப்படை உள்ளீட்டு எண்ணிலிருந்து கணக்கிடப்பட்ட மதிப்பு.

ஹாஷிங் தீர்வுநெறி (செயல்பாடு)
இலக்கமுறை கையொப்பங்கள், செய்தி அங்கீக ாரக் குறியீடுக ள் (MAC-கள்) மற்றும் பிற அங்கீகாரங்களை உருவாக்க ம ற்றும் சரிபார்க்கப் பயன்படுத்தப்படும் ஒரு நிலை அளவில ான ஹா ஷுக்கு தன்னிச்சை அளவிலான தரவையை வரைபடப்படுத்தும் கணிதத் தீர்வுநெறி.

Homomorphic மைறயக்கம்
மறைகுறியாக்கப்பட்ட தகவல்களை முதலில் மறைவிலக்கம் செய்யாமல் கணக்கீடுகளைச் செய்யும் முறை.

மாறாத்தன்மை
(நிரலாக்கத்தில்) ஒரு பொருளை உருவாக்கிய பின் அதை மாற்ற முடியாத நிலை.

உள்ளீடு (MimbleWimble)
பரிவர்த்தனையை அனு ப்பும் தரப்பினரைக் குறிக்கும் MimbleWi mble பரிவர்த்தனையின் கூறு; முந்தைய பரிவர்த்தனைகளின் வெளியீடுகளிலிருந்து உருவாக்கப்பட்டது.

I/O
உள்ளீடு/ வெளியீடு; கணினி போன்ற ஒரு தகவல் செய லாக்க அமைப்புக்கும் மனிதன் அல்லது மற்றொரு தகவல் செயலாக்க அமைப்பு போன்ற வெளி உலகதிற்கும் இடையேயான தொடர்பு.

[15] http://mathworld.wolfram.com/BipartiteGraph.html

[16] Macdonald, Andrew, ***Grin Coin and MimbleWimble: An Introductory Guide***, 18 October, 2018, https://cryptobriefing.com/grin-coin-mimblewimble-introduction/

அதிகபட்ச வழங்கீடு எட்டப்பட வேண்டிய Epic-ன் அளவு, இதற்கு மேல் புழக்கத்திலுள்ள வழங்கீடு அதிகரிக்காது (21,000,000 Epic).

Memory-Hard நிறைய RAM-களை பயன்படுத்தி ஒரே மாதிரியான இணைப்புகளின் இயக்கும் முயற்சிகளைத் தடுக்கிறது. Memory-hard செயல்பாடுகள் தீர்வுநெறிகளாகும், அவற்றின் கணக்கீட்டு நேரங்களை தரவை வைத்திருக்ககூடிய நினைவாகத்தால் தீர்மானிக்கப்படுகின்றன. நினைவக-பிணைப்பு செயல்பாடுகள் என்றும் அழைக்கப்படுகிறது.

Merkle Tree கணினி அறிவியல் பயன்பாடுகளில் பயன்படுத்தப்படும் தரவு அமைப்பு. பிளாக்செயின்களில், Merkle tree-க்கள் பெரிய தரவு கட்டமைப்புகளின் உள்ளடக்கங்களை திறமையாகவும் பாதுகாப்பாகவும் சரிபார்க்க அனுமதிக்கின்றன.

MimbleWimble Bitcoin டெவலப்பர்களின் அரட்டை அறையில் Tom Elvis Jedusor என அறியப்படும் ஒரு புனைப்பெயர் பங்களிப்பாளரால் முன்வைக்கப்பட்ட ஒரு நெறிமுறை.

Multisignature ஒரு இலக்கமுறை கையொப்பத் திட்டம், இது பயனர்களின் குழுவை ஒரு ஆவணத்தில் ஒப்பமிட அனுமதிக்கிறது. வழக்கமாக, multisignature தீர்வுநெறி ஒரு கூட்டு கையொப்பத்தை உருவாக்குகிறது, இது அனைத்து பயனர்களிடமிருந்தும் பெறப்படும் தனித்துவமான ஒப்பங்களின் தொகுப்பைக் காட்டிலும் மிகச் சுருக்கமானது[17].

முனை ஒரு பிளாக்செயின் பிணையத்துடன் இணைக்கவும் பிணையத்தில் உள்ள பிற முனைகளுக்கு பரிவர்த்தனைகள் மற்றும் தொகுதிகள் பற்றிய தகவல்களை ஒரு P2P முறையில் விநியோகிக்கும் ஒரு கணினி.

One Way Aggregate Signature (OWAS) ஒரு பரிவர்த்தனை கையொப்பம் மறைக்குரியக்கப்பட்ட பல கையொப்பங்களைக் கொண்டது , அவற்றின் ஒரு பகுதியான தனிப்பட்ட கையொப்பங்களை கணக்கிடுவது மிகவும் கடினம்.

வெளியீடு (MimbleWimble) பரிவர்த்தனையின் ரசீதைக் குறிக்கும் ஒரு MimbleWimble பரிவர்த்தனையின் கூறு; அடுத்தடுத்த பரிவர்த்தனைகளுக்கு உள்ளீடுகளாகப் பயன்படுத்தப்படுகிறது.

Pedersen Commitment Scheme ஒரு பழமையான மறைகுறியீட்டு முறை, ஒரு நிரூபிப்பவரை எந்தவொரு தகவலையும் வெளிப்படுத்தாமலும், தேர்ந்தெடுக்கப்பட்ட மதிப்பில் ஈடுபட அனுமதிக்கிறது.

தனியார் விசை ஒரு தனியார் விசை என்பது குறியீட்டின் ஒரு சிறிய பாகமாகும், இது உரையை மறையாக்கம் மற்றும் மறைவிலக்கம் செய்யும் தீர்வுநெறிகளை அமைப்பதற்கான பொது விசையுடன் இணைக்கப்பட்டுள்ளது. இது சமச்சீரற்ற விசை மறையாக்கத்தின் போது பொது விசை குறியாக்கவியலின் ஒரு பகுதியாக உருவாக்கப்பட்டது மேலும் ஒரு செய்தியை மறைவிலக்கம் செய்து படிக்கக்கூடிய வடிவத்திற்கு மாற்ற பயன்படுகிறது.

Proof of Work (PoW) தரவின் ஒரு பகுதி உற்பத்தி செய்வது கடினம் (விலை உயர்ந்தது மற்றும் நேரத்தை எடுத்துக்கொள்வது), ஆனால் மற்றவர்களுக்கு சரிபார்க்க எளிதானதாகவும் சில தேவைகளை பூர்த்தி செய்வதாகவும் உள்ளது. வேலைக்கான சான்றுகள் பெரும்பாலும் மறைகுறியீட்டுநாணயங்களின் தொகுதி உருவாக்கத்தில் பயன்படுத்தப்படுகின்றன.

பொது விசை சமச்சீரற்ற விசை மறையாக்க தீர்வுநெறிகளைப் பயன்படுத்தும் பொது விசை மறையாக்க குறியாக்கவியலால் பொது விசை உருவாக்கப்படுகிறது. ஒரு செய்தியை படிக்க முடியாத வடிவமாக மாற்ற பொது விசைகள் பயன்படுத்தப்படுகின்றன.

RAM (சீரற்ற அணுகல் நினைவகம்) இயங்குதளம் (OS), பயன்பாட்டு நிரல்கள் மற்றும் தற்போதைய பயன்பாட்டில் உள்ள தரவு ஆகியவை வைக்கப்பட்டுள்ள ஒரு கணித்தல் சாதனத்திலுள்ள விரைவான அணுகலுடைய தரவு சேமிப்பக சில்லுகள், எனவே அவற்றை சாதனத்தின் செயலியால் விரைவாக அடைய முடியும்.

வரம்புச்சான்று ஒரு பரிவர்த்தனை உள்ளீடுகளின் தொகை பரிவர்த்தனை வெளியீடுகளின் தொகையை விட அதிகமாக உள்ளதா எனவும் அனைத்து பரிவர்த்தனை மதிப்புகளும் நேர்நமறையானவை என்பதை சரிபார்க்கும் செயல்திட்ட சரிபார்ப்பு. வரம்புச்சான்றுகள் நாணய வழங்கீட்டை சேதப்படுத்தாதவாறு உறுதி செய்கிறது.

(இலக்கமுறை) ஒப்பம் பிளாக்செயின் நெறிமுறையின் ஒரு நிலையான பகுதி, பரிவர்த்தனைகள் மற்றும் பரிவர்த்தனைகளின் தொகுதிகளை பாதுகாக்க, தகவல்களை பரிமாற்றம் செய்தல், ஒப்பந்த மேலாண்மை மற்றும் எந்தவொரு வெளிப்புற சேதத்தையும் கண்டறிந்து தடுக்க பயன்படுகிறது. பிளாக்செயினில் தகவல்களை சேமித்தும் மாற்றுவதும் மூன்று விதமான நன்மைகளை வழங்குகின்றன:

- அனுப்பப்படும் தரவு சேதமடைந்துள்ளதா என்பதை அவை வெளிப்படுத்துகின்றன;
- பரிவர்த்தனையில் ஒரு குறிப்பிட்ட தரப்பின் பங்கேற்பை சரிபார்க்கிறது;
- சட்டப்பூர்வமாக பிணைக்கப்படலாம்.

SRAM (நிலையான சீரற்ற அணுகல் நினைவகம்) மின்சாரம் வழங்கப்படும் வரை தரவு பாகங்களை அதன் நினைவகத்தில் வைத்திருக்கும் சீரற்ற அணுகல் நினைவகம் (RAM).

செய்வீதம் கொடுக்கப்பட்டுள்ள மறைகுறியீட்டுநாணய நெறிமுறையால் ஒரு வினாடியில் செய்யக்கூடிய பரிவர்த்தனைகளின் அளவு.

நம்பிக்கையின்மை ஒரு மறைகுறியீட்டுநாணய பிணையத்தின் தரம் ஒரு நெறிமுறையின் விதிகளை ஒரு மத்திய அமைப்பால் அமல்படுத்தப்படாமல் பின்பற்ற வேண்டும்.

[17] Bellare, Mihir, Neven, Gregory, 2007, *Identity-based Multi-signatures from RSA*, Lecture Notes in Computer Science vol. 4377, https://link.springer.com/chapter/10.1007%2F11967668_10

EPIC CASH

EPIC PRIVATE INTERNET CASH