ബിറ്റ്കോയിൻ: ഒരു പിയർടുപിയർ ഇലക്ട്രോണിക് ക്യാഷ് സിസ്റ്റം

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org
Translated in Malayalam by Er Neeludan (linkedin) aka Hyder Ali Abdulla from Bitcoin.org

രത്നച്ചുരുക്കം. ഇലക്ട്രോണിക് പണത്തിന്റെ പിയർടുപിയർ പതിപ്പ് ഒരു സാമ്പത്തിക സ്ഥാപനത്തിലൂടെ അല്ലാതെ ഓൺലൈനിൽ പണമിടപാടുകൾ ഒരു കക്ഷിയിൽ നിന്ന് മറ്റൊന്നിലേക്ക് നേരിട്ട് അയക്കും. ഡിജിറ്റൽ സിഗ്നേച്ചറുകൾ പരിഹാരത്തിന്റെ ഒരു ഭാഗം നൽകുന്നു, പക്ഷേ ഇരട്ടച്ചെലവ് തടയാൻ വിശ്വസനീയമായ ഒരു മൂന്നാം കക്ഷി ആവശ്യമാണെങ്കിൽ പ്രധാന ആനുകൂല്യങ്ങൾ നഷ്ടപ്പെടും. പിയർടുപിയർ നെറ്റ്വർക്ക് ഉപയോഗിച്ച് ഇരട്ടചെലവ് പ്രശ്നത്തിന് ഞങ്ങൾ ഒരു പരിഹാരം നിർദ്ദേശിക്കുന്നു. ഹാഷ് അടിസ്ഥാനമാക്കിയുള്ള പ്രൂഫ്ഓഫ്വർക്ക് ഉപയോഗിച്ച് ഒരു ശൃംഖലയിലേക്ക് ഹാഷ് ചെയ്തുകൊണ്ട് നെറ്റ്വർക്ക് ഇടപാടുകൾ ടൈംസ്റ്റാമ്പ് ചെയ്യുന്നു,പ്രൂഫ് ഓഫ് വർക്ക് വീണ്ടും ചെയ്യാതെ മാറ്റാൻ കഴിയാത്ത ഒരു റെക്കോർഡ് ഉണ്ടാക്കുന്നു . ഏറ്റവും ദൈർഘ്യമേറിയ ശൃംഖല അതിന്റെ ക്രമത്തിന്റെ സംഭവങ്ങൾ സാക്ഷ്യം വഹിച്ചു തെളിവായി മാത്രമല്ല പ്രവർത്തിക്കുന്നത്, പക്ഷേ അതിന്റെ തെളിവാണ് സിപിയു പവറിന്റെ ഏറ്റവും വലിയ പൂളിൽ നിന്നാണ് വന്നതെന്നുള്ളത് .എത്രത്തോളം നെറ്റ്വർക്കിനെ ആക്രമിക്കാൻ സഹകരിക്കാത്ത നോഡുകൾ സിപിയു പവറിന്റെ ഭൂരിഭാഗവും നിയന്ത്രിക്കുന്നുവോ , അവർ ഏറ്റവും ദൈർഘ്യമേറിയ ശൃംഖല സൃഷ്ടിക്കുകയും ആക്രമണകാരികളെ മറികടക്കുകയും ചെയ്യുന്നു.നെറ്റ്വർക്കിന് തന്നെ കുറഞ്ഞ ഘടനയുടെ ആവശ്യമേയുള്ളു. ഒരു മികച്ച ശ്രമത്തിന്റെ അടിസ്ഥാനത്തിലാണ് സന്ദേശങ്ങൾ പ്രക്ഷേപണം ചെയ്യുന്നത്, കൂടാതെ നോഡുകൾക്ക് ഇഷ്ടാനുസരണം നെറ്റ്വർക്കിൽ നിന്ന് പുറത്തുപോകാനും വീണ്ടും ചേരാനും കഴിയും, അവർ പോയപ്പോൾ സംഭവിച്ചതിന്റെ തെളിവായി ഏറ്റവും ദൈർഘ്യമേറിയ പ്രൂഫ്ഓഫ്വർക്ക് ചെയിൻ സ്വീകരികുന്നതിലൂടെ.

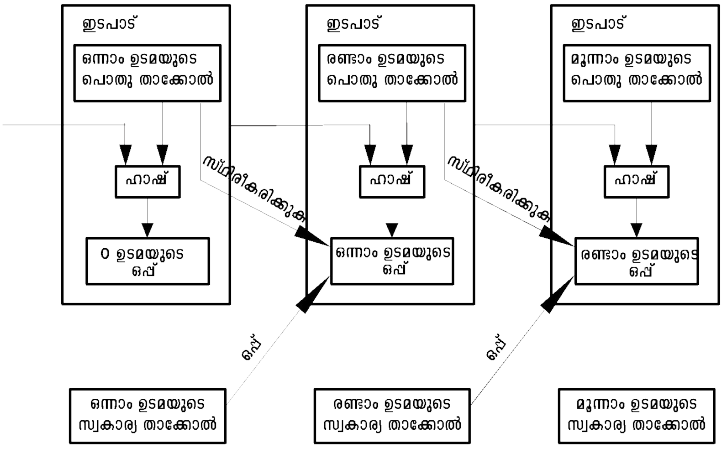
1. ആമുഖം

ഇൻറർനെറ്റിലെ വാണിജ്യം വിശ്വസനീയമായ മൂന്നാം കക്ഷികളായ ധനകാര്യ സ്ഥാപനങ്ങളെയാണ് ഏതാണ്ട് പൂർണ്ണമായും ഇലക്ട്രോണിക് പേയ്മെന്റുകൾ പ്രോസസ്സ് ചെയ്യുന്നതിന് ആശ്രയിക്കുന്നത് .സിസ്റ്റം മിക്ക ഇടപാടുകളിലും നന്നായി പ്രവർത്തിക്കുമ്പോൾ, വിശ്വാസ അധിഷ്ഠിത മോഡലിന്റെ അന്തർലീനമായ ബലഹീനതകൾ അത് ഇപ്പോഴും അനുഭവിക്കുന്നു. സാമ്പത്തിക സ്ഥാപനങ്ങൾക്ക് തർക്കങ്ങളിൽ മധ്യസ്ഥത ഒഴിവാക്കാൻ സാധ്യമല്ലാത്തതിനാൽ, പൂർണ്ണമായും തിരിച്ചെടുക്കാനാവാത്ത ഇടപാടുകൾ യഥാർത്ഥത്തിൽ സാധ്യമല്ല . മധ്യസ്ഥതയുടെ ചെലവ് ഇടപാട് ചെലവ് വർധിപ്പിക്കുകയും കുറഞ്ഞ പ്രായോഗിക ഇടപാട് വലുപ്പം പരിമിതപ്പെടുത്തുകയും ചെറിയ കാഷ്വൽ ഇടപാടുകൾക്കുള്ള സാധ്യത വെട്ടികുറക്കുകയും ചെയ്യുന്നു ,കൂടാതെ നോൺ റിവേഴ്സിബിൾ സേവനങ്ങൾക്ക് നോൺ റിവേഴ്സിബിൾ പേയ്മെന്റുകൾ നടത്താനുള്ള കഴിവ് നഷ്ടപ്പെടുന്നതിന് വിശാലമായ ചിലവുണ്ട്. വിപരീത സാധ്യതയോടെ, വിശ്വാസത്തിന്റെ ആവശ്യകത വ്യാപിക്കുന്നു. വ്യാപാരികൾ നിർബന്ധമായും അവരുടെ ഉപഭോക്താക്കളെ സൂക്ഷിക്കുക, അവർക്ക് ആവശ്യമുള്ളതിനേക്കാൾ കൂടുതൽ വിവരങ്ങൾക്കായി അവരെ ബുദ്ധിമുട്ടിക്കുക. വഞ്ചനയുടെ ഒരു നിശ്ചിത ശതമാനം ഒഴിവാക്കാനാവാത്തതായി അംഗീകരിക്കപ്പെടുന്നു. ഈ ചെലവുകളും പേയ്മെന്റ് അനിശ്ചിതത്വങ്ങളും ഫിസിക്കൽ കറൻസി ഉപയോഗിച്ച് വ്യക്തിപരമായി ഒഴിവാക്കാം, എന്നാൽ പേയ്മെന്റുകൾ ഒരു ആശയവിനിമയ ചാനലിലൂടെ നടത്തുന്നതിന് ഒരു വിശ്വസനീയ കക്ഷി ഇല്ലാതെ ഒരു സംവിധാനവും നിലവിലില്ല .

എന്താണ് വേണ്ടതെന്ന് വച്ചാൽ വിശ്വാസത്തിന് പകരം ക്രിപ്റ്റോഗ്രാഫിക് പ്രൂഫിനെ അടിസ്ഥാനമാക്കിയുള്ള ഒരു ഇലക്ട്രോണിക് പേയ്മെന്റ് സംവിധാനമാണ്, വിശ്വസ്തരായ മൂന്നാം പാർട്ടിയുടെ ആവശ്യമില്ലാതെ പരസ്പരം നേരിട്ട് ഇടപാട് നടത്താൻ തയ്യാറുള്ള രണ്ട് കക്ഷികളെ അനുവദിക്കുന്നു. കണക്കുകൂട്ടലനുസരിച്ച് അപ്രായോഗികമായ ഇടപാടുകൾ തിരിച്ചെടുക്കുന്നത് വിൽപ്പനക്കാരെ വഞ്ചനയിൽ നിന്ന് സംരക്ഷിക്കും , വാങ്ങുന്നവരെ സംരക്ഷിക്കുന്നതിന് സാധാരണ എസ്ക്രോ മെക്കാനിസങ്ങൾ എളുപ്പത്തിൽ നടപ്പിലാക്കാൻ കഴിയും. ഈ പേപ്പറിൽ, ഇടപാടുകളുടെ കാലക്രമ ക്രമത്തിന്റെ കമ്പ്യൂട്ടേഷണൽ തെളിവ് സൃഷ്ടിക്കുന്നതിനുള്ള വിതരണം ചെയ്ത പിയർടുപിയർന്റെ ടൈംസ്റ്റാമ്പ് സെർവർ ഉപയോഗിച്ച് ഇരട്ടച്ചെലവ് പ്രശ്നത്തിന് ഞങ്ങൾ ഒരു പരിഹാരം നിർദ്ദേശിക്കുന്നു. സിസ്റ്റം സത്യസന്ധമായ നോഡുകൾ ഒന്നിച്ച് കൂടുതൽ സിപിയു പവർ നിയന്ത്രിക്കുന്നിടത്തോളം ആക്രമണകാരി നോഡുകളുടെ സഹകരണ സംഘത്തെക്കാളും സുരക്ഷിതമാണ് .

2. ഇടപാടുകൾ

ഡിജിറ്റൽ ഒപ്പുകളുടെ ഒരു ശൃഖലയായി ഞങ്ങൾ ഒരു ഇലക്ട്രോണിക് നാണയത്തെ നിർവചിക്കുന്നു. ഓരോ ഉടമയും നാണയം കൈമാറുമ്പോൾ മുമ്പത്തെ ഇടപാടിന്റെ ഹഷും അടുത്ത ഉടമയുടെ പൊതു താക്കോലും ഡിജിറ്റലായി ഒപ്പിടുന്നതിലൂടെ അടുത്ത നാണയത്തിന്റെ അറ്റത്തു ഇവ ചേർക്കപെടുന്നു. ഉടമസ്ഥാവകാശത്തിലൂടെ ഒരു പണമടക്കുന്നയാൾക് ചെയിൻ പരിശോധിച്ച് ഒപ്പുകൾ പരിശോധിക്കാൻ കഴിയും.

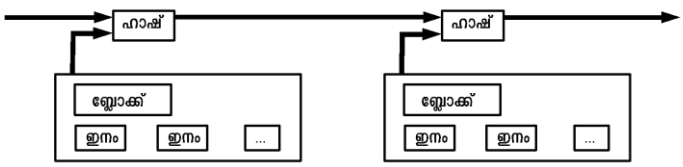


ഉടമകളിലൊരാൾ ഇരട്ടി നാണയതുക ചെലവഴിച്ചിട്ടില്ലെന്ന് സ്ഥിരീകരിക്കാൻ പണമടയ്ക്കുന്നയാൾക്ക് കഴിയില്ല എന്നതാണ് പ്രശ്നം. എല്ലാം പരിശോധിക്കുന്ന ഒരു വിശ്വസനീയമായ കേന്ദ്ര അധികാരം അല്ലെങ്കിൽ മിന്റ് അവതരിപ്പിക്കുക എന്നതാണ് ഒരു ഇരട്ടച്ചെലവിനുള്ള ഇടപാടിന്റെ പൊതു പരിഹാരം. ഓരോ ഇടപാടിനും ശേഷം, നാണയം മിന്റിലേക്ക് തിരികെ നൽകണം ഒരു പുതിയ നാണയം ഇഷ്യൂ ചെയ്യുക, മിന്റിൽ നിന്ന് നേരിട്ട് ഇഷ്യൂ ചെയ്യുന്ന നാണയങ്ങൾ മാത്രം ഇരട്ടി ചിലവഴിക്കില്ലെന്ന് വിശ്വസിക്കപ്പെടുന്നു. ഈ പരിഹാരത്തിന്റെ പ്രശ്നം മുഴുവൻ പണ വ്യവസ്ഥയുടെയും വിധിയെ ആശ്രയിച്ചിരിക്കുന്നു എന്നതാണ് മിന്റ് നടത്തുന്ന കമ്പനി, എല്ലാ ഇടപാടുകളും ഒരു ബാങ്ക് പോലെ അവയിലൂടെ കടന്നുപോകേണ്ടതുണ്ട്.

മുൻ ഉടമകൾ ഇടപാടുകൾ നേരത്തെ ഒപ്പിട്ടിട്ടില്ലെന്ന് പണം സ്വീകരിക്കുന്നയാൾക്ക് അറിയാൻ നമ്മൾക്ക് ഒരു മാർഗം ആവശ്യമാണ്. നമ്മളുടെ ആവശ്യങ്ങൾക്ക്, ഏറ്റവും മുമ്പത്തെ ഇടപാട് പ്രധാനമാണ്, അതിനാൽ പിന്നീട് ഇരട്ടി ചെലവാക്കാനുള്ള ശ്രമങ്ങളെക്കുറിച്ച് നമ്മൾ അത് കാര്യമാക്കുന്നില്ല. ഇടപാടിന്റെ അഭാവം സ്ഥിരീകരിക്കാനുള്ള ഒരേയൊരു മാർഗ്ഗം എല്ലാ ഇടപാടുകളെയും കുറിച്ച് അറിഞ്ഞിരിക്കുക. മിന്റിന് അടിസ്ഥാനമാക്കിയുള്ള മോഡലിൽ, എല്ലാ ഇടപാടുകളെക്കുറിച്ചും ആദ്യം വന്നത് ഏതാണെന്നതിനെക്കുറിച്ചും മിന്റിന് അറിയാമായിരുന്നു. ഒരു വിശ്വസ്ത കക്ഷി ഇല്ലാതെ ഇത് പൂർത്തിയാക്കാൻ, ഇടപാടുകൾ ആയിരിക്കണം പരസ്യമായി പ്രഖ്യാപിക്കണം [1], പങ്കെടുക്കുന്നവർക്ക് അവ സ്വീകരിച്ച ക്രമം ഒരൊറ്റ ചരിത്രത്തെ അംഗീകരിക്കാൻ നമ്മൾക്ക് ഒരു സംവിധാനം ആവശ്യമാണ്. പണം സ്വീകരിക്കുന്നയാൾക്ക് ഓരോ ഇടപാടിന്റെ സമയത്തും തെളിവ് ആവശ്യമാണ് ഭൂരിഭാഗം നോഡുകളും ഇത് ആദ്യം സ്വീകരിച്ചതാണെന്ന് സമ്മതിക്കണം.

3. ടൈം സ്റ്റാമ്പ് സെർവർ

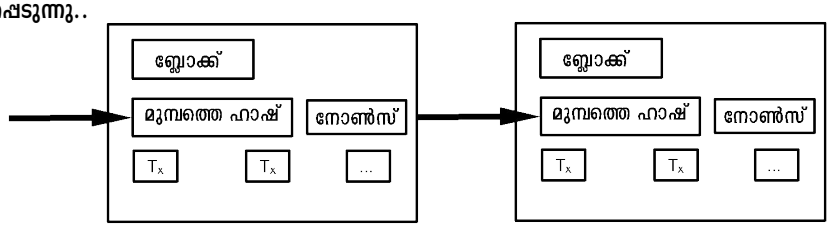
ഞങ്ങൾ നിർദ്ദേശിക്കുന്ന പരിഹാരം ഒരു ടൈംസ്റ്റാമ്പ് സെർവറിൽ ആരംഭിക്കുന്നു. ഒരു ടൈംസ്റ്റാമ്പ് സെർവർ ടൈംസ്റ്റാമ്പ് ചെയ്യേണ്ട ഇനങ്ങളുടെ ഒരു ബ്ലോക്കിന്റെ ഹാഷ്, പത്രം അല്ലെങ്കിൽ യൂസ്നെറ്റ് പോസ്റ്റ് [2-5]. ൽ ഡാറ്റ നിലനിന്നിരുന്നിരിക്കണം എന്ന് ടൈംസ്റ്റാമ്പ് തെളിയിക്കുന്നു സമയം, വ്യക്തമായും, ഹാഷിൽ പ്രവേശിക്കാൻ വേണ്ടി ഹാഷ് വ്യാപകമായി പ്രസിദ്ധീകരിക്കുന്നു. ഓരോ ടൈംസ്റ്റാമ്പിലും മുമ്പത്തെ ടൈംസ്റ്റാമ്പ് ഉൾപ്പെടുന്നു അതിന്റെ ഹാഷ്, ഒരു ചെയിൻ രൂപപ്പെടുത്തുന്നു, ഓരോ അധിക ടൈംസ്റ്റാമ്പും അതിന് മുമ്പുള്ളവയെ ശക്തിപ്പെടുത്തുന്നു.



4. ജോലിയുടെ തെളിവ് അഥവാ പ്രൂഫ് ഓഫ് വർക്ക്

പിയർടുപിയർ അടിസ്ഥാനത്തിൽ വിതരണം ചെയ്ത ടൈംസ്റ്റാമ്പ് സെർവർ നടപ്പിലാക്കാൻ, ഞങ്ങൾ ഒരു തെളിവ് ഉപയോഗിക്കേണ്ടതുണ്ട്. ന്യൂസ്പേപ്പർ അല്ലെങ്കിൽ യൂസ്നെറ്റ് പോസ്റ്റുകൾക്ക് പകരം ആദം ബാക്കിന്റെ ഹാഷ്കാഷ് [6] പോലെയുള്ള വർക്ക് സിസ്റ്റം ഉപയോഗിച്ച്. ഒരു മൂല്യത്തിനായി സ്കാൻ ചെയ്യുന്നത് ജോലിയുടെ തെളിവ്(പ്രൂഫ്ഓഫ്വർക്ക്) ഉൾപ്പെടുന്നു (സെക്യൂർ ഹാഷ് അൽഗോരിതം) SHA-256 പോലെയുള്ള ഹാഷ് ചെയ്യുമ്പോൾ, നിരവധി പൂജ്യം ബിറ്റുകളിൽ നിന്നാണ് ഹാഷ് ആരംഭിക്കുന്നത്. ആവശ്യമുള്ള ശരാശരി ജോലി സംഖ്യയിൽ ക്രമാതീതമായ മാറ്റാം ആയിട്ടുള്ള പൂജ്യം ബിറ്റുകൾ ആവശ്യമാണ്, ഒരൊറ്റ ഹാഷ് നിർവഹനം ചെയ്ത് പരിശോധിക്കാവുന്നതാണ്.

ഞങ്ങളുടെ ടൈംസ്റ്റാമ്പ് നെറ്റ്വർക്കിനായി, ഒരു നോൺസ് വർദ്ധിപ്പിച്ചുകൊണ്ട് ഞങ്ങൾ പ്രൂഫ്ഓഫ്വർക്ക് നടപ്പിലാക്കുന്നു ബ്ലോക്കിന്റെ ഹാഷിന് ആവശ്യമായ പൂജ്യം ബിറ്റുകൾ നൽകുന്ന ഒരു മൂല്യം കണ്ടെത്തുന്നതുവരെ തടയുക. ഒരിക്കൽ സി. പി. യു പ്രൂഫ് ഓഫ്വർക്ക് തൃപ്തിപ്പെടുത്താൻ ശ്രമിച്ചു, ജോലി വീണ്ടും ചെയ്യാതെ ബ്ലോക്ക് മാറ്റാൻ കഴിയില്ല . പിന്നീടുള്ള ബ്ലോക്കുകൾ അതിനു ശേഷം ചങ്ങലയിട്ടതിനാൽ, ബ്ലോക്ക് മാറ്റാനുള്ള ജോലി അതിനു ശേഷമുള്ള എല്ലാ ബ്ലോക്കുകളും വീണ്ടും ചെയ്യുന്നത് പോലെ ഉൾപ്പെടുന്നു..



ഭൂരിപക്ഷ തീരുമാനനിർമ്മാണത്തിലെ പ്രാതിനിധ്യം നിർണ്ണയിക്കുന്നതിനുള്ള പ്രശ്നവും പ്രൂഫ്ഓഫ്വർക്ക് പരിഹരിക്കുന്നു. ഭൂരിപക്ഷം ഒരു ഐപി വിലാസം ഒരു വോട്ട് അടിസ്ഥാനമാക്കിയെങ്കിൽ, അത് ആർക്കും അട്ടിമറിച്ചു നിരവധി ഐപികൾ അനുവദിക്കാൻ കഴിയും. പ്രൂഫ്ഓഫ്വർക്ക് അടിസ്ഥാനപരമായി ഒരുസിപിയുവൺവോട്ട് ആണ്. ഭൂരിപക്ഷം ഏറ്റവും ദൈർഘ്യമേറിയ ശൃംഖലയാണ് തീരുമാനത്തെ പ്രതിനിധീകരിക്കുന്നത്, അതിൽ ഏറ്റവും വലിയ പ്രൂഫ്ഓഫ്വർക്ക് നിക്ഷേപമുണ്ട് . സിപിയു പവറിന്റെ ഭൂരിഭാഗവും സത്യസന്ധമായ നോഡുകളാൽ നിയന്ത്രിക്കപ്പെടുകയാണെങ്കിൽ, സത്യസന്ധമായ ശൃംഖല വേഗതയോടെ വളരുകയും മത്സരിക്കുന്ന ശൃംഖലയെ മറികടക്കുകയും ചെയ്യും . ഒരു മുൻ ബ്ലോക്ക് പരിഷ്ക്കരിക്കുന്നതിന്, ഒരു ആക്രമണകാരി ബ്ലോക്കിന്റെയും അതിനു ശേഷമുള്ള എല്ലാ ബ്ലോക്കുകളുടെയും പ്രൂഫ്ഓഫ്വർക്ക് വീണ്ടും ചെയ്യേണ്ടി വരും, തുടർന്ന് സത്യസന്ധമായ നോഡുകളുടെ പ്രവർത്തനം പിടികൂടി മറികടക്കുകയും വേണം. ഞങ്ങൾ പിന്നീട് കാണിക്കും വേഗത കുറഞ്ഞ ആക്രമണകാരി പിടിക്കപ്പെടാനുള്ള സാധ്യത തുടർന്നുള്ള ബ്ലോക്കുകൾ ചേർക്കുമ്പോൾ ക്രമാതീതമായി കുറയുന്നു.

ഹാർഡ് വെയർ വേഗത വർധിപ്പിക്കുന്നതിനുള്ള പരിഹാരത്തിനും, കാലക്രമേണ നോഡുകൾ പ്രവർത്തിപ്പിക്കുന്നതിനുള്ള വ്യത്യസ്ത താൽപര്യത്തിനുള്ള പരിഹാരത്തിനും,പ്രൂഫ്ഓഫ്വർക്ക് ബുദ്ധിമുട്ട് നിർണ്ണയിക്കുന്നത് ശരാശരി ബ്ലോക്കുകൾ ഇത്ര മണിക്കൂറിൽ ലക്ഷ്യം വച്ചുള്ള ചലിക്കുന്ന ശരാശരിയാണ്. അവ വളരെ വേഗത്തിൽ ജനറേറ്റുചെയ്യുകയാണെങ്കിൽ, ബുദ്ധിമുട്ട് വർദ്ധിക്കുന്നു.

5. നെറ്റ്വർക്ക്

നെറ്റ്വർക്ക് പ്രവർത്തിപ്പിക്കുന്നതിനുള്ള ഘട്ടങ്ങൾ ഇപ്രകാരമാണ്:

1) പുതിയ ഇടപാടുകൾ എല്ലാ നോഡുകളിലേക്കും പ്രക്ഷേപണം ചെയ്യുന്നു.
2) ഓരോ നോഡും ഒരു ബ്ലോക്കിലേക്ക് പുതിയ ഇടപാടുകൾ ശേഖരിക്കുന്നു.
3) ഓരോ നോഡും അതിന്റെ ബ്ലോക്കിന് ബുദ്ധിമുട്ടുള്ള പ്രൂഫ്ഓഫ്വർക്ക് കണ്ടെത്തുന്നതിൽ പ്രവർത്തിക്കുന്നു.
4) ഒരു നോഡ് ഒരു പ്രൂഫ്ഓഫ്വർക്ക് കണ്ടെത്തുമ്പോൾ, അത് എല്ലാ നോഡുകളിലേക്കും ബ്ലോക്ക് പ്രക്ഷേപണം ചെയ്യുന്നു.
5) അതിലെ എല്ലാ ഇടപാടുകളും സാധുതയുള്ളതും ഇതിനകം ചെലവഴിച്ചിട്ടില്ലെങ്കിൽ മാത്രമേ നോഡുകൾ ബ്ലോക്ക് സ്വീകരിക്കുകയുള്ളൂ.
6) ബ്ലോക്കിന്റെ സ്വീകാര്യത നോഡുകൾ പ്രകടിപ്പിക്കുന്നു, അതിൽ അടുത്ത ബ്ലോക്ക് സൃഷ്ടിക്കുന്നതിൽ പ്രവർത്തിക്കുന്നു ചെയിൻ, മുമ്പത്തെ ഹാഷായി സ്വീകരിച്ച ബ്ലോക്കിന്റെ ഹാഷ് ഉപയോഗിക്കുന്നു.

നോഡുകൾ എല്ലായ്പ്പോഴും ഏറ്റവും ദൈർഘ്യമേറിയ ശൃംഖലയെ ശരിയായ ഒന്നായി കണക്കാക്കുകയും അതിനോട് തുടർന്നു പ്രവർത്തിച്ചു അത് നീട്ടുകയും ചെയ്യുന്നു. രണ്ട് നോഡുകൾ ഒരേസമയം അടുത്ത ബ്ലോക്കിന്റെ വ്യത്യസ്ത പതിപ്പുകൾ പ്രക്ഷേപണം ചെയ്താൽ, ചിലത് നോഡുകൾക്ക് ആദ്യം ഒന്നോ മറ്റോ ലഭിച്ചേക്കാം. അങ്ങനെയെങ്കിൽ, അവർ ആദ്യം ലഭിച്ചതിൽ പ്രവർത്തിക്കുന്നു, എന്നാൽ മറ്റേ ശാഖ നീളം കൂടുന്നുണ്ടെങ്കിൽ സംരക്ഷിക്കുകയും ചെയ്യുന്നു . അടുത്ത പ്രൂഫ് ഓഫ് വർക്ക് ലഭിക്കുമ്പോൾ ചങ്ങല ഭേദിക്കപ്പെടുകയും , ഒരു ശാഖ നീളമുള്ളതാകുന്നു; മറ്റൊന്നിൽ പ്രവർത്തിക്കുന്ന നോഡുകൾ പിന്നീട് ദൈർഘ്യമേറിയ ശാഖയിലേക്ക് മാറും.

പുതിയ ഇടപാട് പ്രക്ഷേപണങ്ങൾ എല്ലാ നോഡുകളിലും എത്തണമെന്നില്ല. അവർ ധാരാളം നോഡുകളിലേക് എത്തുന്നിടത്തോളം കാലം , അവ വളരെ മുമ്പുതന്നെ ഒരു ബ്ലോക്കിൽ പ്രവേശിക്കും. പ്രക്ഷേപണം ചെയ്ത ബ്ലോക്ക് ഇട്ട്കളയുന്ന സന്ദേശങ്ങളെ സഹിക്കുന്നു. ഒരു നോഡിന് ഒരു ബ്ലോക്ക് ലഭിച്ചില്ലെങ്കിൽ, അടുത്ത ബ്ലോക്ക് ലഭിക്കുമ്പോൾ അത് അഭ്യർത്ഥിക്കുന്നത് വഴി, അത് ഒരെണ്ണം നഷ്ടമായി എന്ന് മനസ്സിലാക്കുന്നു.

6. പ്രചോദനം

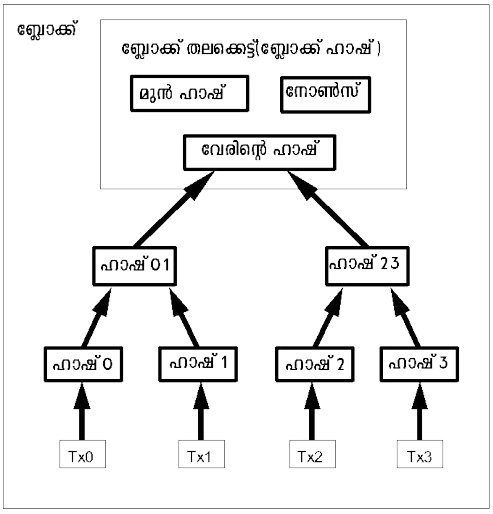
ഉടമ്പടി പ്രകാരം, ഒരു ബ്ലോക്കിലെ ആദ്യത്തെ ഇടപാട് ഒരു പ്രത്യേക ഇടപാടാണ് ബ്ലോക്കിന്റെ സ്രഷ്ടാവിന്റെ ഉടമസ്ഥതയിൽ ഒരു പുതിയ നാണയം ലഭിക്കുന്നത് വഴിയാണ്. ഇത് നെറ്റ്വർക്കിനെ പിന്തുണയ്ക്കുന്നതിന് നോഡുകൾക്ക് ഒരു പ്രോത്സാഹനവും നൽകുന്നു, അവ വിതരണം ചെയ്യാൻ കേന്ദ്ര അധികാരമില്ലാത്തതിനാൽ നാണയങ്ങൾ വിതരണം ചെയ്യുന്നതിനുള്ള തുടക്കത്തിൽ ഒരു മാർഗം കൂടിയാണ്, .പുതിയ നാണയങ്ങളുടെ സ്ഥിരമായ തുകയുടെ സ്ഥിരമായ കൂട്ടിച്ചേർക്കൽ സ്വർണ്ണം പ്രചരിപ്പിക്കുന്നതിന് വേണ്ടി വിഭവങ്ങൾ സ്വർണ്ണ ഖനിത്തൊഴിലാളികൾ ചെലവഴിക്കുന്നതിന് സമാനമാണ്. ഞങ്ങളുടെ കാര്യത്തിൽ, ഇത് സി പി യു സമയവും വൈദ്യുതിയുമാണ് ചെലവഴിക്കുന്നത്.

പ്രചോദനത്തിന്റെ നിക്ഷേപം കൂടി പണമിടപാട് കൂലിക്കൊപ്പം ചെയ്യാനും കഴിയും. ഒരു ഇടപാടിന്റെ ഫലത്തിന്റെ മൂല്യം അതിന്റെ നിക്ഷേപിച്ചതിന്റെ മൂല്യത്തേക്കാൾ കുറവാണെങ്കിൽ , അതിന്റെ ഇടപാട് ഫീ വ്യത്യാസം അതെ ഇടപാട് അടങ്ങുന്ന ബ്ലോക്കിന്റെ പ്രോത്സാഹന മൂല്യത്തിലേക്ക് ചേർക്കുന്നു. പരിസഞ്ചാരണത്തിലേക്കു മുൻകൂട്ടി നിശ്ചയിച്ച നാണയങ്ങളുടെ എണ്ണം വന്നുകഴിഞ്ഞാൽ , പ്രോത്സാഹനം പൂർണ്ണമായും ഇടപാട് ഫീസിലേക്ക് മാറുകയും പണപ്പെരുപ്പം പൂർണമായും മാറുകയും ചെയ്യും.

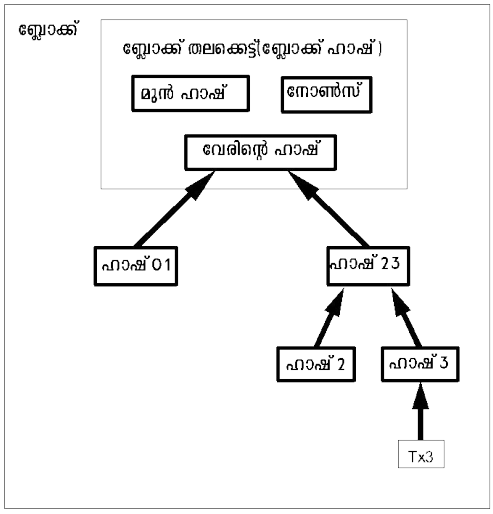
സത്യസന്ധത പുലർത്താൻ നോഡുകളെ പ്രോത്സാഹിപ്പിക്കാൻ പ്രോത്സാഹനം സഹായിച്ചേക്കാം. അത്യാഗ്രഹിയായ ഒരു ആക്രമണകാരിക്ക് കൂടുതൽ സിപിയു ഉപയോഗിച്ച് എല്ലാ സത്യസന്ധമായ നോഡുകളേക്കാളും പവർ കൂട്ടിച്ചേർകാൻ കഴിയുമെങ്കിൽ , അവൻ അത് ഉപയോഗിക്കുന്നതിന് ഇടയിൽ അവന്റെ പേയ്മെന്റുകൾ മോഷ്ടിച്ചുകൊണ്ട് ആളുകളെ കബളിപ്പിക്കുക, അല്ലെങ്കിൽ പുതിയ നാണയങ്ങൾ സൃഷ്ടിക്കാൻ അത് ഉപയോഗിക്കുക എന്നിവ തിരഞ്ഞെടുക്കേണ്ടതുണ്ട്. അത്തരം നിയമങ്ങൾ അവനു കൂടുതൽ നാണയങ്ങൾ മറ്റുള്ളവരെ താരതമ്യം ചെയ്ത് സ്വന്തം സമ്പത്തിന്റെ വ്യവസ്ഥയെയും സാധുതയെയും തുരങ്കം വയ്ക്കുന്നതിനേക്കാൾ ലഭിക്കാൻ അനുകൂലിക്കും.

7. ഡിസ്ക് സ്ഥലം വീണ്ടെടുക്കുന്നു

ഒരു നാണയത്തിലെ ഏറ്റവും പുതിയ ഇടപാട് മതിയായ ബ്ലോക്കുകളിൽ അടക്കിക്കഴിഞ്ഞാൽ, ഡിസ്കിന്റെ സ്ഥലം ലാഭിക്കുന്നതിനായി മുമ്പ് ചെലവഴിച്ച ഇടപാടുകൾ ഉപേക്ഷിക്കാവുന്നതാണ്. ബ്ലോക്കിന്റെ ഹാഷ് തകർക്കാതെ ഇത് സുഗമമാക്കുന്നതിന്, ഇടപാടുകൾ ഒരു മെർക്കിൾ ട്രീയിൽ ഹാഷ് ചെയ്യുന്നു [7][2][5], ബ്ലോക്കിന്റെ ഹാഷിൽ വേരുകൾ മാത്രം ഉൾപ്പെടുത്തിയിരിക്കുന്നു. പിന്നീട് മരത്തിന്റെ ശിഖരങ്ങൾ വെട്ടിമാറ്റി പഴയ ബ്ലോക്കുകൾ ഒതുക്കാവുന്നതാണ്. ഇന്റീരിയർ ഹാഷുകൾ പിന്നീട് സൂക്ഷിക്കേണ്ടതില്ല.



ഇടപാടുകൾ നടത്തുന്നതിന്റെ ഒരു മെർക്കൽ മരം

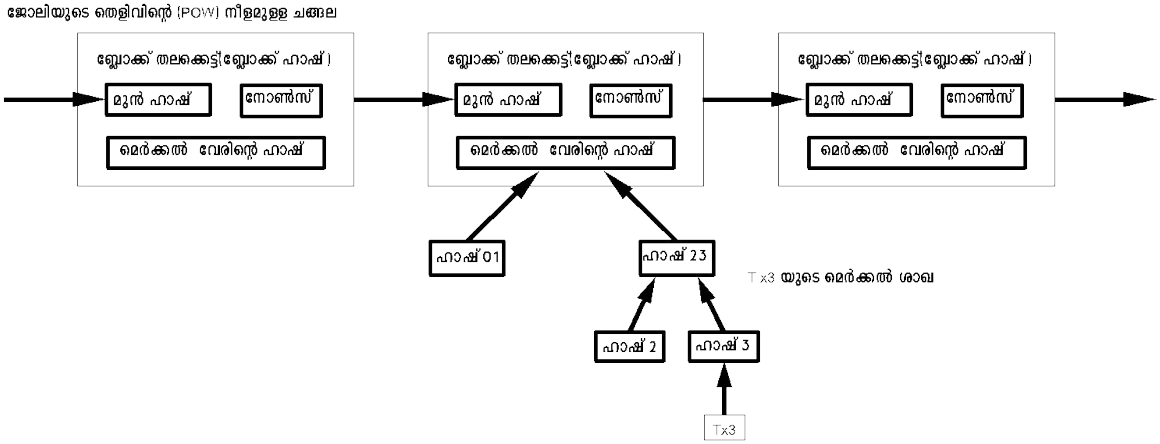


ബ്ലോക്കിൽ നിന്ന് T x0-2 വെട്ടിമാറ്റിയ ശേഷം

ഇടപാടുകളില്ലാത്ത ഒരു ബ്ലോക്ക് തലക്കെട്ട് ഏകദേശം 80 ബൈറ്റുകൾ ആയിരിക്കും. ബ്ലോക്കുകൾ ഓരോ 10 മിനിറ്റിലും ജനറേറ്റുചെയ്യുന്നു എന്ന് നമ്മൾ കരുതുന്നുവെങ്കിൽ, പ്രതിവർഷം 80 ബൈറ്റുകൾ * 6 * 24 * 365 = 4.2MB. കമ്പ്യൂട്ടർ സംവിധാനങ്ങൾക്കൊപ്പം 2008ലെ കണക്കനുസരിച്ച് സാധാരണയായി 2GB RAM ഉപയോഗിച്ച് വിൽക്കുന്നു, കൂടാതെ മൂറിന്റെ നിയമം പ്രതിവർഷം 1.2GB നിലവിലെ വളർച്ച പ്രവചിക്കുന്നു , ബ്ലോക്ക് ഹെഡറുകൾ നിർബന്ധമായും മെമ്മറികളിൽ സൂക്ഷിക്കേണ്ടതുണ്ടെങ്കിൽപ്പോലും സംഭരണം ഒരു പ്രശ്നമാകരുത്.

8. ലളിതമാക്കിയ പേയ്മെന്റ് പരിശോധന

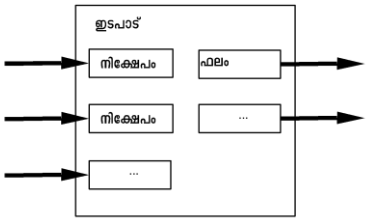
ഒരു പൂർണ്ണ നെറ്റ്വർക്ക് നോഡ് പ്രവർത്തിപ്പിക്കാതെ തന്നെ പേയ്മെന്റുകൾ പരിശോധിക്കുന്നത് സാധ്യമാണ്. ഒരു ഉ പയോക്താവ് ഏറ്റവും ദൈർഘ്യമേറിയ പ്രൂഫ്ഓഫ്വർക്ക് ശൃംഖലയുടെ ബ്ലോക്ക് ഹെഡറുകളുടെ ഒരു പകർപ്പ് സൂക്ഷിച്ചാൽ മതി, അത് അയാൾക്ക് നെറ്റ്വർക്ക് നോഡുകൾ ചോദ്യം ചെയ്യുന്നതിലൂടെ തനിക്ക് ഏറ്റവും നീളമേറിയ ശൃംഖല ഉണ്ടെന്ന് ബോധ്യപ്പെടുകയും ചെയ്യും, ബ്ലോക്കിലേക്ക് ഇടപാടിനെ ലിങ്ക് ചെയ്യുന്ന ടൈംസ്റ്റാമ്പ് ഉള്ള മെർക്കൽ ബ്രാഞ്ച് ലഭിക്കുകയും ചെയ്യും. അയാൾക്ക് സ്വയം ഇടപാട് പരിശോധിക്കാൻ കഴിയില്ല , പക്ഷേ അത് ശൃംഖലയിലെ ഒരു സ്ഥലവുമായി ലിങ്ക് ചെയ്യുന്നതിലൂടെ, ഒരു നെറ്റ്വർക്ക് നോഡ് അത് സ്വീകരിച്ചതായി അയാൾക്ക് കാണാൻ കഴിയും, അതിനുശേഷം ചേർത്ത ബ്ലോക്കുകൾ നെറ്റ്വർക്ക് അത് അംഗീകരിച്ചുവെന്ന് കൂ ടുതൽ സ്ഥിരീകരിക്കുകയും ചെയ്യും.



അതുപോലെ, സത്യസന്ധമായ നോഡുകൾ നെറ്റ്വർക്കിനെ നിയന്ത്രിക്കുന്നിടത്തോളം സ്ഥിരീകരണം വിശ്വസനീയമാണ്, പക്ഷേ ഒരു ആക്രമണകാരി കൂടുതൽ നെറ്റ്വർക്കിനെ കീഴടക്കിയാൽ ദുർബലമാകും. നെറ്റ്വർക്ക് നോഡുകൾക്ക് തങ്ങൾക്കുവേണ്ടിയുള്ള ഇടപാടുകൾ പരിശോധിക്കാൻ കഴിയുമ്പോൾ,ഒരു ആക്രമണകാരിക്ക് നെറ്റ്വർക്കിനെ മറികടക്കാൻ കഴിയു ന്നിടത്തോളം ആക്രമണകാരി കെട്ടിച്ചമച്ചതിലൂടെ ഇടപാടുകൾ ലളിതമാക്കിയ രീതി കബളിപ്പിക്കപ്പെടാം . ഒരു തന്ത്രം നെറ്റ്വർക്ക് നോഡുകളിൽ അസാധുവായതായ ബ്ലോക്ക് കണ്ടെത്തുമ്പോൾ അവയിൽ നിന്നുള്ള അലേർട്ടുകൾ സ്വീകരിക്കുന്നതാണ് ഇതിനെതിരെ പരിരക്ഷിക്കുവാൻ ചെയ്യുക, ഫുൾ ബ്ലോക്ക് ഡൗൺലോഡ് ചെയ്യാൻ ഉപയോക്താവിന്റെ സോഫ്റ്റ്വെയറിനെ പ്രേരിപ്പിക്കുകയും ഇടപാടുകൾ അലേർട്ട് ചെയ്യുകയും പൊരുത്തക്കേട് സ്ഥിരീകരിക്കുകയും ചെയ്യുന്നു. ഇടയ്ക്കിടെ – പേയ്മെന്റുകൾ ലഭിക്കുന്ന ബിസിനസുകൾ ഒരുപക്ഷേ ഇപ്പോഴും ആഗ്രഹിച്ചേക്കാം അവരുടെ സ്വന്തം നോഡുകൾ പ്രവർത്തിപ്പിക്കുക വഴി കൂടുതൽ സ്വതന്ത്രമായ സുരക്ഷയ്ക്കും വേഗത്തിലുള്ള സ്ഥിരീകരണത്തിനും വേണ്ടി.

9. മൂല്യം സംയോജിപ്പിക്കുകയും വിഭജിക്കുകയും ചെയ്യുക

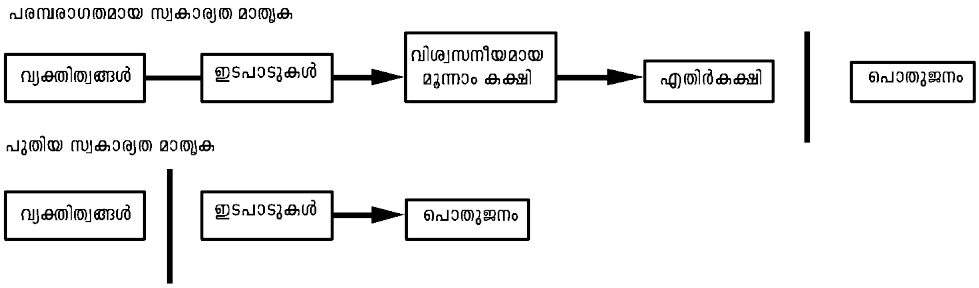
നാണയങ്ങൾ വ്യക്തിഗതമായി കൈകാര്യം ചെയ്യാൻ കഴിയുമെങ്കിലും,ഒരു കൈമാറ്റത്തിലെ ഓരോ സെന്റിനും പ്രത്യേക ഇ ടപാട് നിർമ്മിക്കുന്നത് ബുദ്ധിമുട്ടാണ് . മൂല്യം വിഭജിക്കാനും സംയോജിപ്പിക്കാനും അനുവദിക്കുന്നതിന്, ഇടപാടുകളിൽ ഒന്നിലധികം നിക്ഷേപങ്ങളും ഫലങ്ങളും അടങ്ങിയിരിക്കണം. സാധാരണയായി ഒറ്റ നിക്ഷേപം ആയിരിക്കും മുമ്പത്തെ ഒരു വലിയ ഇടപാടിൽ നിന്നോ ചെറിയ തുകകൾ സംയോജിപ്പിക്കുന്ന ഒന്നിലധികം നിക്ഷേപങ്ങളിൽ നിന്നോ പരമാവധി രണ്ട് ഫലങ്ങൾ: പ്രതിഫലത്തിനായി ഒ ന്ന്, ബാക്കി ചില്ലറ ഇവ ഏതെങ്കിലും ഉണ്ടെങ്കിൽ അത് അയച്ചയാളിലേക്ക് തിരികെ നൽകുന്നു.



ഫാൻ ഔട്ട് എന്നത് ശ്രദ്ധിക്കേണ്ടതാണ്, ഒരു ഇടപാട് നിരവധി ഇടപാടുകളെ ആശ്രയിച്ചിരിക്കുന്നു, ആ ഇടപാടുകൾ പലതിനെയും ആശ്രയിച്ചിരിക്കുന്നു, ഇത് ഇവിടെ ഒരു പ്രശ്നമല്ല. ഒരു ഇടപാടിന്റെ ചരിത്രത്തിന്റെ പൂർണ്ണമായ ഒറ്റപ്പെട്ട പകർപ്പ് വേർതിരിച്ചു ചെയ്യേണ്ട ആവശ്യമില്ല.

10. സ്വകാര്യത

പരമ്പരാഗത ബാങ്കിംഗ് മോഡൽ, ഉൾപ്പെട്ടിരിക്കുന്ന കക്ഷികൾക്കും വിശ്വസനീയമായ മൂന്നാം കക്ഷികൾക്കും വിവരങ്ങളിലേക്കുള്ള പ്രവേശനം പരിമിതപ്പെടുത്തുന്നതിലൂടെ സ്വകാര്യതയുടെ ഒരു തലം കൈവരിക്കുന്നു. എല്ലാ ഇടപാടുകളും പരസ്യമായി പ്രഖ്യാപിക്കേണ്ടതിന്റെ ആവശ്യകത ഈ രീതി ഒഴിവാക്കുന്നു, എന്നാൽ മറ്റൊരു സ്ഥലത്തു വിവരങ്ങളുടെ ഒഴുക്ക് തകർത്തുകൊണ്ട് സ്വകാര്യത നിലനിർത്താനാകും : പൊതു താക്കോലുകൾ അജ്ഞാതമായി സൂക്ഷിക്കുന്നതിലൂടെ. മറ്റൊരാൾക്കുള്ള തുക ആരോ അയക്കുന്നത് പൊതുജനത്തിന് കാണാന്കഴിയും, എന്നാൽ ഇടപാടിനെ ആരുമായും ബന്ധിപ്പിക്കുന്ന വിവരങ്ങളില്ലാതെ. ഇത് സ്റ്റോക്ക് എക്സ്ചേഞ്ചുകൾ പുറത്തുവിടുന്ന വിവരങ്ങളുടെ നിലവാരത്തിന് സമാനമാണ്, എന്നാൽ കക്ഷികൾ ആരാണെന്ന് പറയാതെ തന്നെ ഇവിടെ വ്യക്തിഗത വ്യാപാരങ്ങൾ എടുക്കുന്ന സമയവും വലുപ്പവും , 'ടേപ്പ്', പരസ്യമാകുകയും ചെയ്യുന്നു.



ഒരു അധിക ഫയർവാൾ എന്ന നിലയിൽ, ഓരോ ഇടപാടിനും ഒരു സാധാരണ ഉടമയുമായി ബന്ധപ്പെടുത്തി ചെയ്യപ്പെടുന്നതിൽ നിന്ന് അവയെ സൂക്ഷിക്കാൻ ഒരു പുതിയ താക്കോൽ ജോഡി ഉപയോഗിക്കണം . ഒന്നിലധികം നിക്ഷേപം ഉപയോഗിച്ച് ചില ഇടപാടുകൾ ബന്ധപ്പെടുത്തുന്നത് ഇപ്പോഴും ഒഴിവാക്കാനാവില്ല , അവരുടെ നിക്ഷേപങ്ങൾ അനിവാര്യമായും ഒരേ ഉടമയുടെ ഉടമസ്ഥതയിലുള്ളതാണെന്ന് വെളിപ്പെടുത്തുന്നു. അപകടസാധ്യത ഒരു കീയുടെ ഉടമയെ വെളിപ്പെടുത്തിയാൽ, ബന്ധപ്പെടുത്തുന്നതിലൂടെ അതേ ഉടമ ചെയ്യുന്ന മറ്റ് ഇടപാടുകൾ വെളിപ്പെടുത്തും.

11. കണക്കുകൂട്ടലുകൾ

സത്യസന്ധതയുടെ ചങ്ങലയേക്കാൾ വേഗത്തിൽ ഒരു ബദൽ ശൃംഖല സൃഷ്ടിക്കാൻ ശ്രമിക്കുന്ന ഒരു ആക്രമണകാരി ചങ്ങലയുടെ സാഹചര്യം ഞങ്ങൾ പരിഗണിക്കുന്നു . ഇത് പൂർത്തീകരിച്ചാലും, അത് സിസ്റ്റത്തെ അനിയന്ത്രിതമായ മാറ്റങ്ങൾക്ക് തുറന്നുകൊടുക്കില്ല, വായുവിൽ നിന്ന് മൂല്യം സൃഷ്ടിക്കുന്നതിനോ ആക്രമണകാരിക്ക് ഒരിക്കലും ചേരാത്ത പണം എടുക്കുന്നതിനോ ആയി . നോഡുകൾ ഒരു അസാധുവായ ഇടപാട് പേയ്മെന്റായി സ്വീകരിക്കാൻ പോകുന്നില്ല, സത്യസന്ധമായ നോഡുകൾ ഒരിക്കലും അവരെ ഉൾക്കൊള്ളുന്ന ഒരു ബ്ലോക്ക് സ്വീകരിക്കില്ല . ഒരു ആക്രമണകാരിക്ക് തിരിച്ചെടുക്കാൻ സ്വന്തം ഇടപാടുകളിലൊന്നിൽ അവൻ അടുത്തിടെ ചെലവഴിച്ച പണം മാറ്റാൻ മാത്രമേ ശ്രമിക്കാനാകൂ .

സത്യസന്ധമായ ശൃംഖലയും ആക്രമണകാരി ശൃംഖലയും തമ്മിലുള്ള ഓട്ടത്തെ ഒരു ദ്വിപദമായ ക്രമരഹിതമായ നടത്തമെന്ന് വിശേഷിപ്പിക്കാം . സത്യസന്ധമായ ശൃംഖല ഒരു ബ്ലോക്ക് കൊണ്ട് വിപുലീകരിക്കുന്നതാണ് വിജയ പരിപാടി, +1 ന്റെ കൂടിയ മുന്നേറ്റം, പരാജയം വിഷയം എന്നത് ആക്രമണകാരിയുടെ ശൃംഖല ഒരു ബ്ലോക്ക് കൊണ്ട് നീട്ടുന്നതാണ്, ഇത് വിടവ് -1 കുറയ്ക്കുന്നു.

തന്നിരിക്കുന്ന കമ്മിയിൽ നിന്ന് ഒരു ആക്രമണകാരി പിടിക്കപ്പെടാനുള്ള സാധ്യത ഒരു ചൂതാട്ടക്കാരന് നശിപ്പിക്കുന്ന പ്രശ്നത്തിനു സമാനമാണ്. അപാര നിക്ഷേപമുള്ള ഒരു ചൂതാട്ടക്കാരൻ ഒന്നുമില്ലായ്മയിൽനിന്ന് ആരംഭിച്ച് ഒരു സാധ്യതയിൽ അനന്തമായ പ്രയത്നങ്ങളിലൂടെ ബ്രേക്ക് ഈവനിൽ(ലാഭമോ നഷ്ടമോ ഇല്ലാത്ത) എത്താൻ കളിക്കുന്നു എന്ന് കരുതുക. അവൻ എപ്പോഴെങ്കിലും ബ്രേക്ക്ഇവനിൽ എത്തുന്നു എന്ന സാധ്യത കണക്കാക്കാം , അല്ലെങ്കിൽ ഒരു ആക്രമണകാരി എപ്പോഴെങ്കിലും സത്യസന്ധമായ ശൃംഖലയെ പിടിക്കുന്നു, ഇനിഷറയുന്ന രീതിയിൽ [8]:

p = ഒരു സത്യസന്ധമായ നോഡ് അടുത്ത ബ്ലോക്ക് കണ്ടെത്താനുള്ള സാധ്യത

q = ആക്രമണകാരി അടുത്ത ബ്ലോക്ക് കണ്ടെത്താനുള്ള സാധ്യത

q_z =പിന്നിലുള്ള z ബ്ലോക്കുകളിൽ നിന്ന് ആക്രമണകാരി എപ്പോഴെങ്കിലും പിടിക്കപ്പെടാനുള്ള സാധ്യത

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

p > q എന്ന ഞങ്ങളുടെ അനുമാനം അനുസരിച്ച്, ബ്ലോക്കുകളുടെ എണ്ണം കൂടുന്നത് പോലെ ആക്രമണകാരിക്കു ആ വർദ്ധനവ് പിടിക്കണം എന്നതിനാൽ സാധ്യത ഗണ്യമായി കുറയുന്നു . അവനെതിരെയുള്ള സാധ്യതകളോടെ, അവൻ നേരത്തെ തന്നെ മുന്നോട്ട് കുതിച്ചു ഭാഗ്യം ചെയ്തില്ലെങ്കിൽ , അവന്റെ അവസരങ്ങൾ അപ്രത്യക്ഷമാകും അവൻ കൂടുതൽ പിന്നിലാകുമ്പോൾ.

ഒരു പുതിയ ഇടപാടിന്റെ സ്വീകർത്താവ് ആകുന്നതിന് മുമ്പ് എത്ര സമയം കാത്തിരിക്കണമെന്ന് അയച്ചയാൾക്ക് ഇടപാട് മാറ്റാൻ കഴിയില്ലെന്ന് ഉറപ്പാണ് എന്ന് ഞങ്ങൾ ഇപ്പോൾ പരിഗണിക്കുന്നു. അയച്ചയാൾ ഒരു ആക്രമണകാരിയാണെന്ന് ഞങ്ങൾ അനുമാനിക്കുന്നു സ്വീകർത്താവിന് താൻ കുറച്ച് സമയത്തേക്ക് പണം നൽകിയെന്ന് വിശ്വസിക്കാൻ ആഗ്രഹിക്കുന്നവർ, കുറച്ച് സമയത്തിന് ശേഷം അത് തിരികെ സ്വയം പിൻവലികനായി മാറ്റുകയും ചെയ്യും. അത് സംഭവിക്കുമ്പോൾ സ്വീകർത്താവിന് മുന്നറിയിപ്പ് നൽകും, പക്ഷേ ഇത് വളരെ വൈകുമെന്ന് അയച്ചയാൾ പ്രതീക്ഷിക്കുന്നു.

സ്വീകരിക്കുന്നവൻ ഒരു പുതിയ കീ ജോഡി ജനറേറ്റ് ചെയ്യുകയും ഒപ്പിടുന്നതിനു കുറച്ച് മുമ്പ് അയച്ചയാൾക്ക് പൊതു കീ നൽകുകയും ചെയ്യുന്നു . ഇത് അയച്ചയാളെ ബ്ലോക്കുകളുടെ ഒരു ശൃംഖല തയ്യാറാക്കുന്നതിൽ നിന്ന് തടയുന്ന ആ നിമിഷം ജോലി ചെയ്യുന്നതിലൂടെ അയാൾക്ക് വേണ്ടത്ര മുന്നോട്ട് പോകാനുള്ള ഭാഗ്യം ലഭിക്കുന്നതുവരെ അത് തുടർച്ചയായി ഇടപാട് നടത്തുന്നു. ഇടപാട് അയച്ചുകഴിഞ്ഞാൽ, സത്യസന്ധമല്ലാത്ത അയച്ചയാൾ അവന്റെ ഇടപാടിന്റെ ഇതര പതിപ്പ് അടങ്ങുന്ന സമാന്തര ശൃംഖല രഹസ്യമായി പ്രവർത്തിക്കാൻ തുടങ്ങുന്നു.

സ്വീകർത്താവ് ഒരു ഇടപാട് ബ്ലോക്കിലേക്ക് ചേർക്കുകയും ൂ ബ്ലോക്കുകൾ ആകുകയും ചെയ്യുന്നതുവരെ കാത്തിരിക്കുന്നു അതിനു ശേഷം ലിങ്ക് ചെയ്തു. ആക്രമണകാരി നടത്തിയ പുരോഗതിയുടെ കൃത്യമായ അളവ് അവനറിയില്ല, പക്ഷേ സത്യസന്ധമായ ബ്ലോക്കുകൾ ഓരോ ബ്ലോക്കിനും ശരാശരി പ്രതീക്ഷിക്കുന്ന സമയമെടുക്കുമെന്ന് കരുതുക, ആക്രമണകാരിയുടെ സാധ്യത പുരോഗതി പ്രതീക്ഷിക്കുന്ന മൂല്യമുള്ള ഒരു വിഷ വിതരണമായിരിക്കും:

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

ആക്രമണകാരിക്ക് ഇപ്പോഴും പിടിക്കാനാകുന്ന സംഭാവ്യത ലഭിക്കാൻ,ആ ഘട്ടത്തിൽ നിന്ന് അയാൾക്ക് പിടിച്ചെടുക്കാൻ സാധിക്കുന്ന സംഭാവ്യതയനുസരിച്ച് അയാൾക്ക് ഉണ്ടാക്കാമായിരുന്ന ഓരോ പുരോഗതിയിലും ഞങ്ങൾ വിഷസാന്ദ്രത വർദ്ധിപ്പിക്കുന്നു:

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

വിതരണത്തിന്റെ അനന്തമായ വാൽ സങ്കലനം ഒഴിവാക്കാൻ പുന:ക്രമീകരിക്കുന്നു...

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

സി കോഡിലേക്ക് പരിവർത്തനം ചെയ്യുന്നു

```
#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;
}
```

ചില ഫലങ്ങൾ പ്രവർത്തിപ്പിക്കുമ്പോൾ, Z ഉപയോഗിച്ച് സാധ്യത കുറഞ്ഞുവരുന്ന വക്താവ് ആയി നമുക്ക് കാണാൻ കഴിയും.

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

0.1% ന് താഴെയുള്ള p ക്ക് പരിഹാരം...

< 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. ഉപസംഹാരം

വിശ്വാസത്തെ ആശ്രയിക്കാതെ ഇലക്ട്രോണിക് ഇടപാടുകൾക്കായി ഒരു സംവിധാനം ഞങ്ങൾ നിർദ്ദേശിച്ചിട്ടുണ്ട്. ഞങ്ങൾ ഡിജിറ്റൽ സിഗ്നേച്ചറുകളിൽ നിന്ന് നിർമ്മിച്ച നാണയങ്ങളുടെ സാധാരണ ചട്ടക്കൂട് തുടങ്ങി , ഉടമസ്ഥാവകാശത്തിനു ഇത് ശക്തമായ നിയന്ത്രണം നൽകുന്നു, എന്നാൽ ഇരട്ടച്ചെലവ് തടയാനുള്ള മാർഗമില്ലാതെ അപൂർണ്ണമാണ്. ഇത് പരിഹരിക്കാൻ, ഞങ്ങൾ ഇടപാടുകളുടെ പൊതു ചരിത്രം രേഖപ്പെടുത്തുന്നതിന് പ്രൂഫ്ഓഫ്വർക്ക് ഉപയോഗിച്ച് ഒരു പിയർടുപിയർ നെറ്റ്വർക്ക് നിർദ്ദേശിച്ചു സത്യസന്ധമായ നോഡുകളാണെങ്കിൽ, ആക്രമണകാരിക്ക് അത് പെട്ടെന്ന് കണക്കുകൂട്ടാൻ സിപിയു പവറിന്റെ ഭൂരിഭാഗവും നിയന്ത്രിക്കുക അപ്രായോഗികമായി മാറും. ശൃംഖല അതിന്റെ ഘടനാരഹിതമായ തെളിമയിൽ ശക്തമാണ്. ചെറിയ ഏകോപനത്തോടെ ഒരേസമയം നോഡുകൾ പ്രവർത്തിക്കും. അവ തിരിച്ചറിയേണ്ടതില്ല, സന്ദേശങ്ങൾ ആയതിനാൽ ഏതെങ്കിലും പ്രത്യേക സ്ഥലത്തേക്ക് വഴിതിരിച്ചുവിട്ടിട്ടില്ല, മികച്ച പ്രയത്നത്തിന്റെ അടിസ്ഥാനത്തിൽ മാത്രമേ വിതരണം ചെയ്യാവൂ. നോഡുകൾക്ക് ഇഷ്ടമുള്ളപ്പോൾ നെറ്റ്വർക്ക് വിടുകയും വീണ്ടും ചേരുകയും ചെയ്യാം,അവർ പോയപ്പോൾ എന്താണ് സംഭവിച്ചത് എന്നുള്ളത് പ്രൂഫ്ഓഫ്വർക്ക് ശൃംഖല സ്വീകരിച്ചത്കൊണ്ട് തെളിവായി.അവരുടെ സിപിയു ശക്തി ഉപയോഗിച്ച് വോട്ടുചെയ്യുന്നു, അവർ തങ്ങളുടെ സ്വീകാര്യത പ്രകടിപ്പിച്ചുകൊണ്ട് സാധുവായ ബ്ലോക്കുകൾ വിപുലീകരിച്ചു പ്രവർത്തിക്കുന്നതിലൂടെയും അവയിൽ പ്രവർത്തിക്കാൻ വിസമ്മതിച്ചുകൊണ്ട് അസാധുവായ ബ്ലോക്കുകൾ നിരസിക്കുന്നു. ഈ സമവായ സംവിധാനം ഉപയോഗിച്ച് ആവശ്യമായ നിയമങ്ങളും പ്രോത്സാഹനങ്ങളും നടപ്പിലാക്കാൻ കഴിയും.

അവലംബങ്ങൾ

[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.