ബിറ്റ്കോയിൻ: ഒരു പിയർ-ടു-പിയർ ഇലക്ട്രോണിക് ക്യാഷ് സിസ്റ്റം

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

Translated in Malayalam from bitcoin.org/bitcoin.pdf by B.Tom

സംഗ്രഹം. ഒരു ശുദ്ധ പിയർ-ടു-പിയർ ഇലക്ട്രോണിക് ക്യാഷ് പതിപ്പ്, ധനകാര്യ സ്ഥാപനത്തിലൂടെ പോകാതെ തന്നെ ഓൺലൈൻ പേയ്മെന്റുകൾ ഒരു കക്ഷിയിൽ നിന്ന് മറ്റൊന്നിലേക്ക് നേരിട്ട് അയയ്ക്കാൻ അനുവദിക്കും. ഡിജിറ്റൽ സിഗ്നേച്ചറുകൾ ഇതിനൊരു ഭാഗിക പരിഹാരം നൽകുന്നു, എന്നാൽ ഡബിൾ-സ്പെൻഡിങ് തടയുന്നതിന് വിശ്വസനീയമായ ഒരു മൂന്നാം കക്ഷി ഇപ്പോഴും ആവശ്യമാണെങ്കിൽ പ്രധാന നേട്ടങ്ങൾ നഷ്ടപ്പെടുന്നു. ഒരു പിയർ-ടു-പിയർ നെറ്റ്വർക്ക് ഉപയോഗിച്ച് ഡബിൾ-സ്പെൻഡിങ് പ്രശ്നത്തിന് പരിഹാരം ഞങ്ങൾ നിർദ്ദേശിക്കുന്നു. നെറ്റ്വർക്ക് ഇടപാടുകളെ ടൈംസ്റ്റാമ്പ് ചെയ്യുന്നതിനായി അവയെ നിലവിലുള്ള ഹാഷ്-അധിഷ്ഠിത പ്രൂഫ്-ഓഫ്-വർക്ക് ചെയിനിലേക്ക് ഹാഷ് ചെയ്ത് പ്രൂഫ്-ഓഫ്-വർക്ക് വീണ്ടും ചെയ്യാതെ മാറ്റാൻ കഴിയാത്ത ഒരു റെക്കോർഡ് സൃഷ്ടിക്കുന്നു. ഏറ്റവും ദൈർഘ്യമേറിയ ചെയിൻ സാക്ഷ്യം വഹിച്ച സംഭവങ്ങളുടെ ശ്രേണിയുടെ തെളിവായി മാത്രമല്ല, സി.പി.യു. ശക്തിയുടെ ഏറ്റവും വലിയ പൂളിൽ നിന്നാണ് വന്നതെന്നതിന്റെ തെളിവായി വർത്തിക്കുന്നു. നെറ്റ്വർക്കിനെ ആക്രമിക്കാൻ സഹകരിക്കാത്ത നോഡുകളാൽ ഭൂരിഭാഗം സി.പി.യു. പവറും നിയന്ത്രിക്കപ്പെടുന്നിടത്തോളം കാലം, അവർ ഏറ്റവും ദൈർഘ്യമേറിയ ചെയിൻ സൃഷ്ടിക്കുകയും ആക്രമണകാരികളെ മറികടക്കുകയും ചെയ്യും. നെറ്റ്വർക്കിന് തന്നെ കുറഞ്ഞ ഘടന മതി. മികച്ച ശ്രമത്തിന്റെ അടിസ്ഥാനത്തിലാണ് സന്ദേശങ്ങൾ പ്രക്ഷേപണം ചെയ്യുന്നത്, കൂടാതെ നോഡുകൾക്ക് ഇഷ്ടാനുസരണം നെറ്റ്വർക്കിൽ നിന്ന് പുറത്തുപോകാനും വീണ്ടും ചേരാനും കഴിയും, ഇല്ലാതിരുന്നപ്പോൾ സംഭവിച്ചതിന്റെ തെളിവായി ഏറ്റവും ദൈർഘ്യമേറിയ പ്രൂഫ്-ഓഫ്-വർക്ക് ചെയിൻ നോഡുകൾ സ്വീകരിക്കുന്നു.

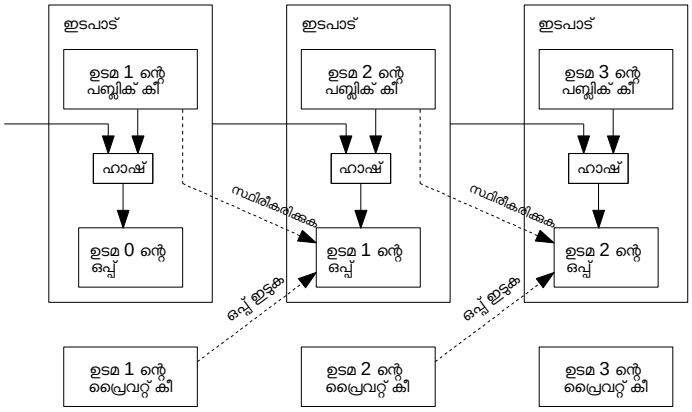
1. ആമുഖം

ഇൻറർനെറ്റിലെ വാണിജ്യം മിക്കവാറും ഇലക്ട്രോണിക് പേയ്മെന്റുകൾ പ്രോസസ്സ് ചെയ്യുന്നതിന് വിശ്വസനീയമായ മൂന്നാം കക്ഷികളായി പ്രവർത്തിക്കുന്ന ധനകാര്യ സ്ഥാപനങ്ങളെ ആശ്രയിച്ചിരിക്കുന്നു. മിക്ക ഇടപാടുകൾക്കും ഈ സിസ്റ്റം നന്നായി പ്രവർത്തിക്കുന്നുണ്ടെങ്കിലും, ട്രസ്റ്റ് അധിഷ്ഠിത മോഡലിന്റെ അന്തർലീനമായ ബലഹീനതകൾ ഇതിൽ ഇപ്പോഴും അനുഭവപ്പെടുന്നു. പൂർണമായും തിരിച്ചെടുക്കാനാവാത്ത ഇടപാടുകൾ ശരിക്കും സാധ്യമല്ല, കാരണം ധനകാര്യ സ്ഥാപനങ്ങൾക്ക് മധ്യസ്ഥ തർക്കങ്ങൾ ഒഴിവാക്കാൻ കഴിയില്ല. മധ്യസ്ഥതയിലുള്ള ചെലവ് ഇടപാട് ചെലവ് വർദ്ധിപ്പിക്കുകയും, കുറഞ്ഞ പ്രായോഗിക ഇടപാട് പരിധി പരിമിതപ്പെടുത്തുകയും, ചെറിയ കാഷ്വൽ ഇടപാടുകൾക്കുള്ള സാധ്യത വെട്ടിക്കുറയ്ക്കുകയും ചെയ്യുന്നു. പഴയപടിയാക്കാനാവാത്ത സേവനങ്ങൾക്കായി റിവേർസിബിൾ അല്ലാത്ത പേയ്മെന്റുകൾ നടത്താനുള്ള കഴിവ് നഷ്ടപ്പെടുന്നതിന് വലിയ വില കൊടുക്കേണ്ടി വരുന്നു. റിവേഴ്സിബിൾ ആക്കാനുള്ള കഴിവ്, വിശ്വാസത്തിന്റെ ആവശ്യകത വർദ്ധിപ്പിക്കുന്നു. വ്യാപാരികൾ അവരുടെ ഉപഭോക്താക്കളെക്കുറിച്ച് ജാഗ്രത പാലിക്കേണ്ടിവരുന്നു, ഉപയോക്താക്കൾ അവർക്ക് ആവശ്യമുള്ളതിനേക്കാൾ കൂടുതൽ വിവരങ്ങൾക്കായി വ്യാപാരികളെ ബുദ്ധിമുട്ടിക്കുന്നു. വഞ്ചനയുടെ ഒരു നിശ്ചിത ശതമാനം ഒഴിവാക്കാനാവില്ലെന്ന് എല്ലാവരും അംഗീകരിക്കുന്നു. ഫിസിക്കൽ കറൻസി ഉപയോഗിച്ച് ഈ ചെലവുകളും പേയ്മെന്റ് അനിശ്ചിതത്വങ്ങളും നേരിടുള്ള ഇടപാടുകളിൽ ഒഴിവാക്കാനാകും, എന്നാൽ വിശ്വസനീയമായ ഒരു കക്ഷിയില്ലാതെ ഒരു ആശയവിനിമയ ചാനലിലൂടെ പേയ്മെന്റുകൾ നടത്തുന്നതിനുള്ള ഒരു സംവിധാനവും നിലവിലില്ല.

വിശ്വാസ്യതയ്ക്ക് പകരം ക്രിപ്റ്റോഗ്രാഫിക് തെളിവ് അടിസ്ഥാനമാക്കിയുള്ള ഒരു ഇലക്ട്രോണിക് പേയ്മെന്റ് സംവിധാനമാണ് വേണ്ടത്, വിശ്വസനീയമായ മൂന്നാം കക്ഷിയുടെ ആവശ്യമില്ലാതെ രണ്ട് സന്നദ്ധരായ കക്ഷികൾ പരസ്പരം നേരിട്ട് ഇടപാട് നടത്താൻ അനുവദിക്കുന്നത്. റിവേഴ്സൽ അപ്രായോഗികമായ ഇടപാടുകൾ വിൽപ്പനക്കാരെ വഞ്ചനയിൽ നിന്ന് സംരക്ഷിക്കും, മാത്രമല്ല വാങ്ങുന്നവരെ പരിരക്ഷിക്കുന്നതിന് പതിവ് എസ്ക്രോ സംവിധാനങ്ങൾ എളുപ്പത്തിൽ നടപ്പിലാക്കാം. ഈ പേപ്പറിൽ, ഇടപാടുകളുടെ കാലക്രമത്തിന്റെ ക്രിപ്റ്റോഗ്രാഫിക് തെളിവ് ഉത്പാദിപ്പിക്കുന്ന ഒരു പിയർ-ടു-പിയർ ഡിസ്ട്രിബ്യൂട്ട് ടൈംസ്റ്റാമ്പ് സെർവർ ഉപയോഗിച്ച് ഇരട്ട-ചെലവ് പ്രശ്നത്തിന് പരിഹാരം ഞങ്ങൾ നിർദ്ദേശിക്കുന്നു. ആക്രമണകാരികളായ നോഡുകളുടെ സഹകരണ ഗ്രൂപ്പുകളേക്കാൾ സത്യസന്ധമായ നോഡുകൾ കൂട്ടായി കൂടുതൽ സി.പി.യു. പവർ നിയന്ത്രിക്കുന്നിടത്തോളം കാലം സിസ്റ്റം സുരക്ഷിതമാണ്.

2. ഇടപാടുകൾ

ഡിജിറ്റൽ ഒപ്പുകളുടെ ഒരു ചെയിൻ ആയി ഞങ്ങൾ ഒരു ഇലക്ട്രോണിക് നാണയത്തെ നിർവചിക്കുന്നു. മുമ്പത്തെ ഇടപാടിന്റെ ഒരു ഹാഷും അടുത്ത ഉടമയുടെ പബ്ലിക് കീയും, ഡിജിറ്റലായി ഒപ്പിട്ട് നാണയത്തിന്റെ അവസാനത്തിൽ ഇവ ചേർത്തുകൊണ്ട് ഓരോ ഉടമയും അടുത്ത ഉടമക്ക് നാണയം കൈമാറുന്നു. ഉടമസ്ഥാവകാശ ചെയിൻ സ്ഥിരീകരിക്കുന്നതിന് ഒരു പണമടയ്ക്കുന്നയാൾക്ക് ഒപ്പുകൾ പരിശോധിക്കുന്നതിലൂടെ കഴിയും.

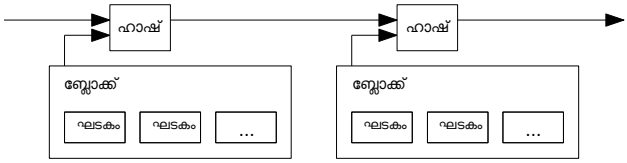


ഉടമസ്ഥരിൽ ഒരാൾ നാണയം ഡബിൾ-സ്പെൻഡ് ചെയ്തിട്ടില്ലെന്ന് സ്ഥിരീകരിക്കാൻ പണമടയ്ക്കുന്നയാൾക്ക് കഴിയില്ല എന്നതാണ് പ്രശ്നം. ഡബിൾ-സ്പെൻഡിങ് ആണോയെന്ന് ഓരോ ഇടപാടുകളും പരിശോധിക്കുന്ന വിശ്വസനീയമായ കേന്ദ്ര അതോറിറ്റി അഥവാ കമ്മട്ടം അവതരിപ്പിക്കുക എന്നതാണ് ഒരു പൊതു പരിഹാരം. ഓരോ ഇടപാടിനും ശേഷം, ഒരു പുതിയ നാണയം നൽകുന്നതിന് നാണയം കമ്മട്ടത്തിലേക്ക് തിരികെ നൽകണം, കൂടാതെ കമ്മട്ടത്തിൽ നിന്ന് നേരിട്ട് നൽകുന്ന നാണയങ്ങൾ മാത്രമേ ഡബിൾ-സ്പെൻഡ് ചെയ്തിട്ടില്ല എന്ന് വിശ്വസിക്കാനാകൂ. ഈ പരിഹാരത്തിലെ പ്രശ്നം, മുഴുവൻ പണ വ്യവസ്ഥയുടെയും വിധി കമ്മട്ടം പ്രവർത്തിപ്പിക്കുന്ന കമ്പനിയെ ആശ്രയിച്ചിരിക്കുന്നു എന്നതാണ്, ഓരോ ഇടപാടുകളും അവയിലൂടെ കടന്നുപോകേണ്ടിവരും, ഒരു ബാങ്ക് പോലെ.

മുമ്പത്തെ ഉടമകൾ നേരത്തെ മറ്റ് ഇടപാടുകളിലൊന്നും ഒപ്പിട്ടിട്ടില്ലെന്ന് പണമടയ്ക്കുന്നയാൾക്ക് അറിയാൻ ഞങ്ങൾക്ക് ഒരു മാർഗം ആവശ്യമാണ്. ഞങ്ങളുടെ ആവശ്യങ്ങൾക്കായി, ആദ്യ ഇടപാട് മാത്രം ആണ് ഞങ്ങൾ കണക്കാക്കുന്നത്, അതിനാൽ ഡബിൾ-സ്പെൻഡ് ചെയ്യാനുള്ള പിന്നീടുള്ള ശ്രമങ്ങളെക്കുറിച്ച് ഞങ്ങൾ ശ്രദ്ധിക്കുന്നില്ല. ഒരു ഇടപാടിന്റെ അഭാവം സ്ഥിരീകരിക്കുന്നതിനുള്ള ഏക മാർഗം എല്ലാ ഇടപാടുകളെക്കുറിച്ചും അറിഞ്ഞിരിക്കുക എന്നതാണ്. കമ്മട്ടം അടിസ്ഥാനമാക്കിയുള്ള മാതൃകയിൽ, കമ്മട്ടം എല്ലാ ഇടപാടുകളെക്കുറിച്ചും ബോധവാന്മാരായിരുന്നു, ഏത് ഇടപാടാണ് ആദ്യം എത്തിയതെന്ന് തീരുമാനിക്കുന്നു. വിശ്വസനീയമായ ഒരു കക്ഷി കൂടാതെ ഇത് നിറവേറ്റുന്നതിന്, ഇടപാടുകൾ പരസ്യമായി പ്രഖ്യാപിക്കണം [1], പങ്കെടുക്കുന്നവർ ലഭിച്ച ക്രമത്തിന്റെ ഒരൊറ്റ ചരിത്രം അംഗീകരിക്കുന്നതിന് ഞങ്ങൾക്ക് ഒരു സംവിധാനം ആവശ്യമാണ്. ഓരോ ഇടപാടിന്റെയും സമയത്ത്, ഭൂരിഭാഗം നോഡുകളും ഇത് ആദ്യം ലഭിച്ച ഇടപാടാണെന്ന് സമ്മതിച്ചതിന് പണമടച്ചയാൾക്ക് തെളിവ് ആവശ്യമാണ്.

3. ടൈംസ്റ്റാമ്പ് സെർവർ

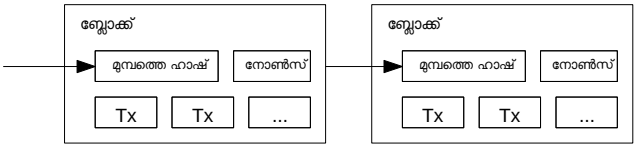
ഞങ്ങൾ നിർദ്ദേശിക്കുന്ന പരിഹാരം ഒരു ടൈംസ്റ്റാമ്പ് സെർവറിൽ ആരംഭിക്കുന്നു. ടൈംസ്റ്റാമ്പ് ചെയ്യേണ്ട ഘടകങ്ങളുടെ ഒരു ബ്ലോക്ക് ഹാഷ് ചെയ്തത് വ്യാപകമായി പ്രസിദ്ധീകരിച്ചുകൊണ്ട് ഒരു ടൈംസ്റ്റാമ്പ് സെർവർ പ്രവർത്തിക്കുന്നു, ഒരു പത്രം അല്ലെങ്കിൽ യൂസ്നെറ്റ് പോസ്റ്റ് പോലെ [2–5]. ഡാറ്റ ഹാഷിൽ ഉൾപെടുന്നതിലൂടെ, ആ സമയത്ത് ഡാറ്റ നിലവിലുണ്ടായിരുന്നുവെന്ന് ടൈംസ്റ്റാമ്പ് തെളിയിക്കുന്നു. ഓരോ ടൈംസ്റ്റാമ്പിലും അതിന്റെ ഹാഷിൽ മുമ്പത്തെ ടൈംസ്റ്റാമ്പ് ഉൾപ്പെടുന്നു, ഒരു ചെയിൻ രൂപപ്പെടുന്നു, ഓരോ അധിക ടൈംസ്റ്റാമ്പും അതിനുമുമ്പുള്ളവയെ ശക്തിപ്പെടുത്തുന്നു.



4. പ്രൂഫ്-ഓഫ്-വർക്ക്

ഒരു പിയർ-ടു-പിയർ അടിസ്ഥാനത്തിൽ വിതരണം ചെയ്ത ടൈംസ്റ്റാമ്പ് സെർവർ നടപ്പിലാക്കാൻ, പത്രം അല്ലെങ്കിൽ യൂസ്നെറ്റ് പോസ്റ്റുകൾക്ക് പകരം ആദം ബാക്കിന്റെ ഹാഷ്കാഷിന് [6] സമാനമായ ഒരു പ്രൂഫ്-ഓഫ്-വർക്ക് സിസ്റ്റം ഞങ്ങൾ ഉപയോഗിക്കേണ്ടതുണ്ട്. SHA-256 പോലുള്ള ഹാഷ് ചെയ്യുമ്പോൾ, നിശ്ചിത പൂജ്യം ബിറ്റുകളിൽ ഹാഷ് ആരംഭിക്കുന്ന മൂല്യത്തിനായി സ്കാൻ ചെയ്യുന്നതാണ് പ്രൂഫ്-ഓഫ്-വർക്ക്. ആവശ്യമായ ശരാശരി വർക്ക്, ആവശ്യമുള്ള പൂജ്യം ബിറ്റുകളുടെ എണ്ണത്തിൽ എക്സ്പോണൻഷ്യൽ ആണ് , ഒരൊറ്റ ഹാഷ് എക്സിക്യൂട്ട് ചെയ്യുന്നതിലൂടെ ഇത് പരിശോധിക്കാൻ കഴിയും.

ഞങ്ങളുടെ ടൈംസ്റ്റാമ്പ് നെറ്റ്വർക്കിനായി, ബ്ലോക്കിന്റെ ഹാഷിന് ആവശ്യമായ പൂജ്യം ബിറ്റുകൾ നൽകുന്ന ഒരു മൂല്യം കണ്ടെത്തുന്നതുവരെ ബ്ലോക്കിൽ ഒരു നോൺസ് ഇൻക്രെമെന്റ് ചെയ്യുന്നു. ഒരിക്കൽ പ്രൂഫ്-ഓഫ്-വർക്ക് തൃപ്തിപ്പെടുത്തുന്നതിനായി സി.പി.യു. ചെലവഴിച്ചുകഴിഞ്ഞാൽ, ഇതേ പ്രവൃത്തി വീണ്ടും ചെയ്യാതെ ബ്ലോക്ക് മാറ്റാൻ കഴിയില്ല. പിന്നീടുള്ള ബ്ലോക്കുകൾ ഒന്നിനു പുറകെ ഒന്നായ് ക്രമത്തിൽ ചേർക്കുന്നതിനാൽ, ഒരു ബ്ലോക്ക് മാറ്റുന്നതിനുള്ള ജോലികളിൽ അതിനുശേഷമുള്ള എല്ലാ ബ്ലോക്കുകളും വീണ്ടും ചെയ്യുന്നത് ഉൾപ്പെടുന്നു.



പ്രൂഫ്-ഓഫ്-വർക്ക് ഭൂരിപക്ഷ തീരുമാനമെടുക്കുന്നതിൽ പ്രാതിനിധ്യം നിർണ്ണയിക്കുന്നതിനുള്ള പ്രശ്നവും പരിഹരിക്കുന്നു. ഭൂരിപക്ഷം ഒരു-ഐ.പി.-വിലാസം-ഒരു-വോട്ട് അടിസ്ഥാനമാക്കിയുള്ളതാണെങ്കിൽ, നിരവധി ഐ.പി. വിലാസങ്ങൾ അനുവദിക്കാൻ കഴിയുന്ന ആർക്കും ഇത് അട്ടിമറിക്കാനാകും. പ്രൂഫ്-ഓഫ്-വർക്ക് അടിസ്ഥാനപരമായി ഒരു-സി.പി.യു.-ഒരു വോട്ട് ആണ്. ഭൂരിപക്ഷ തീരുമാനത്തെ പ്രതിനിധീകരിക്കുന്നത് ഏറ്റവും ദൈർഘ്യമേറിയ ചെയിൻ ആണ്, അതിൽ ഏറ്റവും വലിയ പ്രൂഫ്-ഓഫ്-വർക്ക് പരിശ്രമമുണ്ട്. ഭൂരിഭാഗം സി.പി.യു. പവറും നിയന്ത്രിക്കുന്നത് സത്യസന്ധമായ നോഡുകളാണെങ്കിൽ, സത്യസന്ധമായ ചെയിൻ അതിവേഗം വളരുകയും മത്സരിക്കുന്ന ചെയ്നുകളെ മറികടക്കുകയും ചെയ്യും. ഒരു പഴയ ബ്ലോക്ക് പരിഷ്ക്കരിക്കുന്നതിന്, ഒരു ആക്രമണകാരിക്ക് ബ്ലോക്കിന്റെയും അതിനുശേഷമുള്ള എല്ലാ ബ്ലോക്കുകളുടെയും പ്രൂഫ്-ഓഫ്-വർക്ക് വീണ്ടും ചെയ്യേണ്ടതുണ്ട്, തുടർന്ന് സത്യസന്ധമായ നോഡുകളുടെ പ്രവർത്തനത്തെ മറികടക്കേണ്ടതുണ്ട്. തുടർന്നുള്ള ബ്ലോക്കുകൾ ചേർത്തുകഴിയുമ്പോൾ വേഗത കുറഞ്ഞ ആക്രമണകാരിയെ വിജയിക്കുവാനുള്ള സാധ്യത ഗണ്യമായി കുറയുന്നുവെന്ന് ഞങ്ങൾ പിന്നീട് കാണിക്കാം.
വർദ്ധിച്ചുവരുന്ന ഹാർഡ്വെയർ വേഗതക്കും, കാലക്രമേണ മാറുന്ന നോഡുകൾ പ്രവർത്തിപ്പിക്കുന്നതിനുള്ള താൽപ്പര്യത്തിനും പരിഹാരം കാണുന്നതിന്, മണിക്കൂറിൽ ബ്ലോക്കുകളുടെ ശരാശരി എണ്ണം അടിസ്ഥാനമാക്കിയുള്ളത ചലിക്കുന്ന ശരാശരിയാണ് പ്രൂഫ്-ഓഫ്-വർക്ക് ബുദ്ധിമുട്ട് നിർണ്ണയിക്കുന്നത്. ബ്ലോക്കുകൾ വളരെ വേഗത്തിൽ ജനറേറ്റുചെയ്യുകയാണെങ്കിൽ, ബുദ്ധിമുട്ട് വർദ്ധിക്കുന്നു.

5. നെറ്റ്വർക്ക്

നെറ്റ്വർക്ക് പ്രവർത്തിപ്പിക്കുന്നതിനുള്ള ഘട്ടങ്ങൾ ഇനിപ്പറയുന്നവയാണ്:

1) പുതിയ ഇടപാടുകൾ എല്ലാ നോഡുകളിലേക്കും പ്രക്ഷേപണം ചെയ്യുന്നു.
2) ഓരോ നോഡും ഒരു ബ്ലോക്കിലേക്ക് പുതിയ ഇടപാടുകൾ ശേഖരിക്കുന്നു.
3) ഓരോ നോഡും അതിന്റെ ബ്ലോക്കിനായി പ്രയാസകരമായ തെളിവ് കണ്ടെത്തുന്നതിനായി പ്രവർത്തിക്കുന്നു.
4) ഒരു നോഡ് പ്രൂഫ്-ഓഫ്-വർക്ക് കണ്ടെത്തുമ്പോൾ, അത് എല്ലാ നോഡുകളിലേക്കും ബ്ലോക്ക് പ്രക്ഷേപണം ചെയ്യുന്നു.
5) ബ്ലോക്കിലെ എല്ലാ ഇടപാടുകളും സാധുതയുള്ളതും ഇതിനകം ചെലവഴിച്ചിട്ടില്ലെങ്കിൽ മാത്രം നോഡുകൾ ബ്ലോക്ക് സ്വീകരിക്കുന്നു.
6) സ്വീകരിച്ച ബ്ലോക്കിന്റെ ഹാഷ് മുമ്പത്തെ ഹാഷായി ഉപയോഗിച്ച് ചെയിനിലെ അടുത്ത ബ്ലോക്ക് സൃഷ്ടിക്കുന്നതിലൂടെ നോഡുകൾ ബ്ലോക്കിന്റെ സ്വീകാര്യത പ്രകടിപ്പിക്കുന്നു.

നോഡുകൾ എല്ലായ്പ്പോഴും ദൈർഘ്യമേറിയ ചെയിനിനെ ശരിയായ ഒന്നായി കണക്കാക്കുന്നു, മാത്രമല്ല അത് വിപുലീകരിക്കുന്നതിന് പ്രവർത്തിക്കുകയും ചെയ്യും. രണ്ട് നോഡുകൾ അടുത്ത ബ്ലോക്കിന്റെ വ്യത്യസ്ത പതിപ്പുകൾ ഒരേസമയം പ്രക്ഷേപണം ചെയ്യുകയാണെങ്കിൽ, ചില നോഡുകൾക്ക് ഏതെങ്കിലുമൊന്ന് ആദ്യം

ലഭിച്ചേക്കാം. അത്തരം സന്ദർഭങ്ങളിൽ, അവർക്ക് ലഭിച്ച ആദ്യത്തേതിൽ അവർ പ്രവർത്തിക്കുന്നു, എന്നാൽ അതോടൊപ്പം മറ്റേ ശാഖ സേവ് ചെയ്യുന്നു. ജോലിയുടെ അടുത്ത തെളിവ് കണ്ടെത്തുകയും ഒരു ശാഖ നീളം കൂടുകയും ചെയ്യുമ്പോൾ ടൈ തകർക്കപ്പെടും; മറ്റേ ശാഖയിൽ പ്രവർത്തിച്ചിരുന്ന നോഡുകൾ പിന്നീട് ദൈർഘ്യമേറിയതിലേക്ക് മാറും.

പുതിയ ഇടപാട് പ്രക്ഷേപണങ്ങൾ എല്ലാ നോഡുകളിലും എത്തിച്ചേരേണ്ട ആവശ്യമില്ല. അവ നിരവധി നോഡുകളിൽ എത്തുന്നിടത്തോളം കാലം അവ ഒരു ബ്ലോക്കിലേക്ക് പ്രവേശിക്കും. ഒരു നോഡിന് ഒരു ബ്ലോക്ക് ലഭിച്ചില്ലെങ്കിൽ, അടുത്ത ബ്ലോക്ക് ലഭിക്കുകയും അത് നഷ്ടപ്പെട്ടുവെന്ന് മനസ്സിലാക്കുകയും ചെയ്യുമ്പോൾ നഷ്ടപ്പെട്ട ബ്ലോക്ക് അത് അഭ്യർത്ഥിക്കും.

6. പ്രോത്സാഹനം

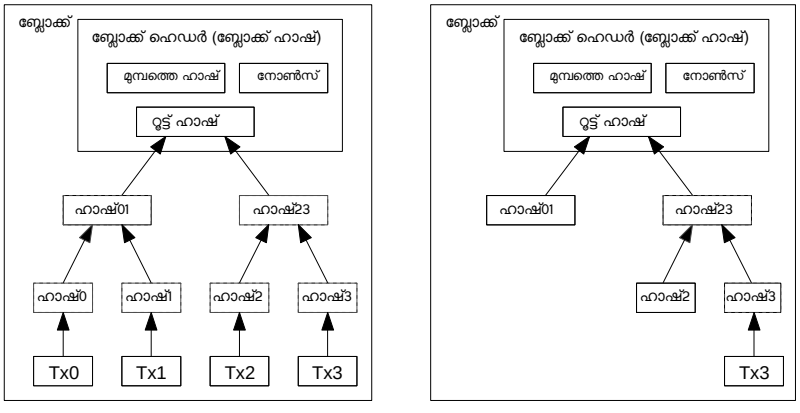
കൺവെൻഷൻ പ്രകാരം, ഒരു ബ്ലോക്കിലെ ആദ്യ ഇടപാട് ഒരു പ്രത്യേക ഇടപാടാണ്, അത് ബ്ലോക്കിന്റെ സ്രഷ്ടാവിന്റെ ഉടമസ്ഥതയിലുള്ള ഒരു പുതിയ നാണയം ആരംഭിക്കുന്നു. ഇത് നെറ്റ്വർക്കിനെ പിന്തുണയ്ക്കുന്നതിന് നോഡുകൾക്ക് ഒരു പ്രോത്സാഹനം നൽകുന്നു, കൂടാതെ നാണയങ്ങൾ വിതരണം ചെയ്യുന്നതിനുള്ള കേന്ദ്ര അതോറിറ്റി ഇല്ലാത്തതിനാൽ തുടക്കത്തിൽ നാണയങ്ങൾ വിതരണം ചെയ്യുന്നതിനുള്ള ഒരു മാർഗ്ഗം നൽകുന്നു. പുതിയ നാണയങ്ങളുടെ സ്ഥിരമായ കൂട്ടിച്ചേർക്കൽ, സ്വർണ്ണ ഖനിത്തൊഴിലാളികൾ സ്വർണ്ണം സർക്കുലേഷനിൽ എത്തിക്കാനായി വിഭവങ്ങൾ ചെലവഴിക്കുന്നതിന് സമാനമാണ്. ഞങ്ങളുടെ കാര്യത്തിൽ, ചെലവഴിക്കുന്നത് സി.പി.യു. സമയവും വൈദ്യുതിയുമാണ്.

ഇടപാട് ഫീസ് ഉപയോഗിച്ചും പ്രോത്സാഹനത്തിന് ധനസഹായം നൽകാം. ഒരു ഇടപാടിന്റെ ഔട്ട്പുട്ട് മൂല്യം അതിന്റെ ഇൻപുട്ട് മൂല്യത്തേക്കാൾ കുറവാണെങ്കിൽ, വ്യത്യാസം ഒരു ഇടപാട് ഫീസാണ്, അത് ഇടപാട് അടങ്ങിയിരിക്കുന്ന ബ്ലോക്കിന്റെ പ്രോത്സാഹന മൂല്യത്തിലേക്ക് ചേർക്കുന്നു. മുൻകൂട്ടി നിശ്ചയിച്ചിട്ടുള്ള നാണയങ്ങളുടെ എണ്ണം സർക്കുലേഷനിൽ പ്രവേശിച്ചുകഴിഞ്ഞാൽ, പ്രോത്സാഹനത്തിന് പൂർണ്ണമായും ഇടപാട് ഫീസിലേക്ക് മാറാനും പൂർണമായും പണപ്പെരുപ്പരഹിതമാവാനും കഴിയും.

സത്യസന്ധമായി തുടരാൻ നോഡുകളെ പ്രോത്സാഹിപ്പിക്കുന്നതിന് പ്രോത്സാഹനം സഹായിച്ചേക്കാം. അത്യാഗ്രഹിയായ ആക്രമണകാരിക്ക് എല്ലാ സത്യസന്ധമായ നോഡുകളേക്കാളും കൂടുതൽ സി.പി.യു. പവർ കൂട്ടിച്ചേർക്കാൻ കഴിയുമെങ്കിൽ, പേയ്മെന്റുകൾ മോഷ്ടിച്ചുകൊണ്ട് ആളുകളെ വഞ്ചിക്കാൻ അത് ഉപയോഗിക്കണോ അല്ലെങ്കിൽ പുതിയ നാണയങ്ങൾ സൃഷ്ടിക്കുന്നതിന് ഉപയോഗിക്കണോ എന്ന് അയാൾക്ക് തിരഞ്ഞെടുക്കേണ്ടതുണ്ട്. വ്യവസ്ഥയെയും സ്വന്തം സമ്പത്തിന്റെ സാധുതയെയും ദുർബലപ്പെടുത്തുന്നതിനേക്കാൾ, അനുകൂലമായ നിയമങ്ങൾ ഉപയോഗിച്ച് മറ്റുള്ളവരെല്ലാം സംയോജിപ്പിച്ചതിനേക്കാൾ കൂടുതൽ പുതിയ നാണയങ്ങൾ സമ്പാദിക്കുന്നത് കൂടുതൽ ലാഭകരമായി അയാൾ കാണേണ്ടതുണ്ട്.

7. ഡിസ്ക് സ്പേസ് വീണ്ടെടുക്കൽ

ഒരു നാണയത്തിലെ ഏറ്റവും പുതിയ ഇടപാടുള്ള ബ്ലോക്ക് മതിയായ ബ്ലോക്കുകൾക്ക് പിന്നിലായികഴിഞ്ഞാൽ, ഡിസ്ക് സ്പേസ് ലാഭിക്കുന്നതിന് മുമ്പ് നടന്ന ഇടപാടുകൾ നീക്കം ചെയ്യാൻ കഴിയും. ബ്ലോക്കിന്റെ ഹാഷ് തകർക്കാതെ ഇത് സുഗമമാക്കുന്നതിന്, ഇടപാടുകൾ ഒരു മെർക്കൽ ട്രീയിൽ ഹാഷ് ചെയ്യുന്നു [7] [2] [5], ബ്ലോക്കിന്റെ ഹാഷിൽ റൂട്ട് മാത്രമേ ഉൾപ്പെടുത്തിയിട്ടുള്ളൂ. വൃക്ഷത്തിന്റെ ശാഖകൾ മുറിച്ചുമാറ്റി പഴയ ബ്ലോക്കുകൾ ചുരുക്കാം. ഇന്റീരിയർ ഹാഷുകൾ സംഭരിക്കേണ്ടതില്ല.



ഇടപാടുകൾ ഒരു മെർക്കൽ ട്രീയിൽ ഹാഷ് ചെയ്തു

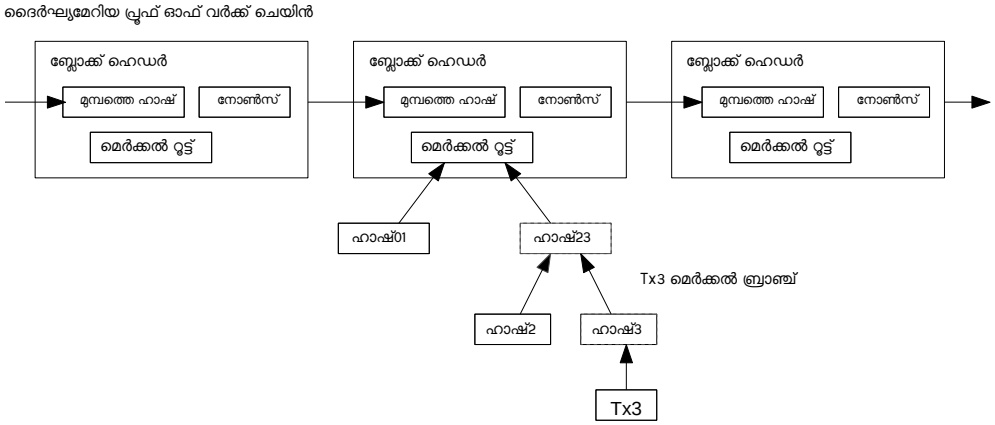
ബ്ലോക്കിൽ നിന്ന് Tx0-2 നീക്കം ചെയ്തതിനു ശേഷം

ഇടപാടുകളില്ലാത്ത ഒരു ബ്ലോക്ക് തലക്കെട്ട് ഏകദേശം 80 ബൈറ്റുകൾ ആയിരിക്കും. ഓരോ 10 മിനിറ്റിലും ബ്ലോക്കുകൾ ജനറേറ്റുചെയ്യുന്നുവെന്ന് കരുതുകയാണെങ്കിൽ, പ്രതിവർഷം 80 ബൈറ്റുകൾ * 6 * 24 * 365 = 4.2

എം.ബി.. 2008 ലെ കണക്കനുസരിച്ച് കമ്പ്യൂട്ടർ സിസ്റ്റങ്ങൾ സാധാരണയായി 2 ജി.ബി. റാമിൽ വിൽക്കുന്നു, മൂർ നിയമവും പ്രതിവർഷം 1.2 ജി.ബി. വളർച്ച പ്രവചിക്കുന്നു, ബ്ലോക്ക് ഹെഡറുകൾ മെമ്മറിയിൽ സൂക്ഷിക്കേണ്ടതുണ്ടെങ്കിലും സംഭരണം ഒരു പ്രശ്നമാകില്ല.

8. ലളിതമായ പേയ്മെന്റ് പരിശോധന

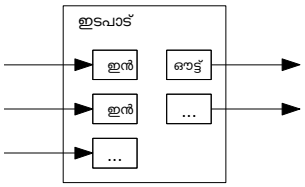
ഒരു പൂർണ്ണ നെറ്റ്വർക്ക് നോഡ് പ്രവർത്തിപ്പിക്കാതെ തന്നെ പേയ്മെന്റുകൾ പരിശോധിക്കാൻ കഴിയും. ഒരു ഉപയോക്താവിന് ഏറ്റവും ദൈർഘ്യമേറിയ പ്രൂഫ്-ഓഫ്-വർക്ക് ചെയിനിന്റെ ബ്ലോക്ക് ഹെഡറുകളുടെ ഒരു പകർപ്പ് സൂക്ഷിച്ചാൽ മതിയാകും, ഉപയോക്താവിന് ഏറ്റവും ദൈർഘ്യമേറിയ ചെയിൻ ലഭിച്ചു എന്ന് ബോധ്യപ്പെടുന്നതുവരെ നെറ്റ്വർക്ക് നോഡുകൾ കൃറി ചെയ്യാനാകും, കൂടാതെ ഇടപാടിനെ ടൈംസ്റ്റാമ്പ് ചെയ്തിരിക്കുന്ന ബ്ലോക്കുമായി ബന്ധിപ്പിക്കുന്ന മെർക്കൽ ബ്രാഞ്ച് കണ്ടുപിടിക്കുക. ഉപയോക്താവിന് ഇടപാട് സ്വയം സ്ഥിരീകരിക്കാൻ കഴിയില്ല, പക്ഷേ അത് ചെയിനിലെ ഒരു സ്ഥലവുമായി ലിങ്കുചെയ്യുന്നതിലൂടെ, ഒരു നെറ്റ്വർക്ക് നോഡ് അത് സ്വീകരിച്ചതായി കാണാൻ കഴിയും, കൂടാതെ അതിനുശേഷം ചേർത്ത ബ്ലോക്കുകൾ നെറ്റ്വർക്ക് അത് അംഗീകരിച്ചതായി സ്ഥിരീകരിക്കുന്നു.



അതുപോലെ, സത്യസന്ധമായ നോഡുകൾ നെറ്റ്വർക്കിനെ നിയന്ത്രിക്കുന്നിടത്തോളം കാലം പരിശോധന വിശ്വസനീയമാണ്, പക്ഷേ ഒരു ആക്രമണകാരി നെറ്റ്വർക്കിനെ കീഴടക്കുകയാണെങ്കിൽ അത് കൂടുതൽ ദുർബലമാകും. നെറ്റ്വർക്ക് നോഡുകൾക്ക് സ്വയം ഇടപാടുകൾ സ്ഥിരീകരിക്കാൻ കഴിയുമെങ്കിലും, ആക്രമണകാരി നെറ്റ്വർക്കിനെ കീഴടക്കി തുടരുന്നിടത്തോളം കാലം ആക്രമണകാരിയുടെ കെട്ടിച്ചമച്ച ഇടപാടുകൾ വഴി ലളിതമായ പരിശോധന രീതിയെ കബളിപ്പിക്കാനാകും. നെറ്റ്വർക്ക് നോഡുകളിൽ നിന്ന് അസാധുവായ ഒരു ബ്ലോക്ക് കണ്ടെത്തുമ്പോൾ അവയിൽ നിന്നുള്ള അലേർട്ടുകൾ സ്വീകരിക്കുകയെന്നതാണ് ഇതിൽ നിന്ന് പരിരക്ഷിക്കുന്നതിനുള്ള ഒരു തന്ത്രം, ഇത് പൊരുത്തക്കേട് സ്ഥിരീകരിക്കുന്നതിന് ഉപയോക്താവിന്റെ സോഫ്റ്റ്വെയറിനെ പൂർണ്ണ ബ്ലോക്കും സംശയകരമായ ഇടപാടുകളും ഡൌൺലോഡ് ചെയ്യാൻ പ്രേരിപ്പിക്കുന്നു. എന്നാലും പതിവ് പേയ്മെന്റുകൾ സ്വീകരിക്കുന്ന ബിസിനസ്സുകൾ കൂടുതൽ സ്വതന്ത്ര സുരക്ഷയ്ക്കും വേഗത്തിലുള്ള സ്ഥിരീകരണത്തിനുമായി സ്വന്തം നോഡുകൾ പ്രവർത്തിപ്പിക്കാൻ ആഗ്രഹിക്കാൻ ഇടയുണ്ട്.

9. മൂല്യത്തിന്റെ സംയോജനവും വിഭജനവും

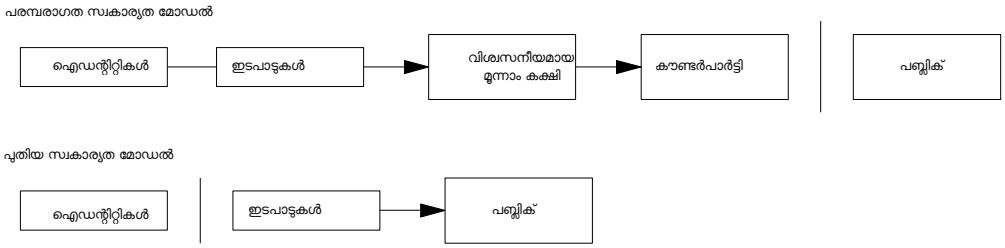
വ്യക്തിഗതമായി നാണയങ്ങൾ കൈകാര്യം ചെയ്യാൻ കഴിയുമെങ്കിലും, ഒരു കൈമാറ്റത്തിലെ ഓരോ സെന്റിനും പ്രത്യേക ഇടപാട് നടത്തുന്നത് ബുദ്ധിമുട്ടാണ്. മൂല്യം വിഭജിക്കാനും സംയോജിപ്പിക്കാനും അനുവദിക്കുന്നതിന്, ഇടപാടുകളിൽ ഒന്നിലധികം ഇൻപുട്ടുകളും ഔട്ട്പുട്ടുകളും അടങ്ങിയിരിക്കുന്നു. സാധാരണയായി മുമ്പത്തെ ഒരു വലിയ ഇടപാടിൽ നിന്നുള്ള ഒരു ഇൻപുട്ട് അല്ലെങ്കിൽ ചെറിയ തുകകൾ സംയോജിപ്പിക്കുന്ന ഒന്നിലധികം ഇൻപുട്ടുകൾ ഉണ്ടാകും, പരമാവധി രണ്ട് ഔട്ട്പുട്ടുകൾ: പേയ്മെന്റിനായി ഒന്ന്, മിച്ചം എന്തെങ്കിലും ഉണ്ടെങ്കിൽ അയച്ചയാൾക്ക് തിരികെ നല്കാൻ മറ്റൊന്ന്.



ഒരു ഇടപാട് നിരവധി ഇടപാടുകളെ ആശ്രയിച്ചിരിക്കുന്ന, കൂടാതെ ആ ഇടപാടുകൾ മറ്റു പല ഇടപാടുകളെ ആശ്രയിച്ചിരിക്കുന്ന ഫാൻ-ഔട്ട് ഇവിടെ ഒരു പ്രശ്നമല്ലെന്ന കാര്യം ശ്രദ്ധിക്കേണ്ടതാണ്. ഒരു ഇടപാടിന്റെ ചരിത്രത്തിന്റെ പൂർണ്ണമായ ഒരു പകർപ്പ് എടുക്കേണ്ട ആവശ്യമില്ല.

10. സ്വകാര്യത

ഉൾപ്പെട്ടിരിക്കുന്ന കക്ഷികൾക്കും വിശ്വസനീയമായ മൂന്നാം കക്ഷിക്കും വിവരങ്ങളിലേക്കുള്ള ആക്സസ്സ് പരിമിതപ്പെടുത്തിക്കൊണ്ട് പരമ്പരാഗത ബാങ്കിംഗ് മോഡൽ സ്വകാര്യത കൈവരിക്കുന്നു. എല്ലാ ഇടപാടുകളും പരസ്യമായി പ്രഖ്യാപിക്കേണ്ടതിന്റെ ആവശ്യകത ഈ രീതിയെ പരസ്യമായി തടയുന്നു, പക്ഷേ മറ്റൊരു സ്ഥലത്ത് വിവരങ്ങളുടെ ഒഴുക്ക് തകർക്കുന്നതിലൂടെ സ്വകാര്യത നിലനിർത്താൻ കഴിയും: പബ്ലിക് കീകൾ അജ്ഞാതമായി സൂക്ഷിക്കുന്നതിലൂടെ. ഒരാൾ മറ്റൊരാൾക്ക് ഒരു തുക അയയ്ക്കുന്നുവെന്ന് പൊതുജനങ്ങൾക്ക് കാണാൻ കഴിയും, എന്നാൽ വിവരങ്ങൾ ആരുമായും ബന്ധിപ്പിക്കുന്നില്ല. ഇത് സ്റ്റോക്ക് എക്സ്ചേഞ്ചുകൾ പുറത്തുവിടുന്ന വിവരങ്ങൾക്ക് സമാനമാണ്, ഇവിടെ വ്യക്തിഗത ട്രേഡുകളുടെ സമയവും വലുപ്പവും ("ടേപ്പ്") പരസ്യപ്പെടുത്തുന്നു, പക്ഷേ കക്ഷികൾ ആരാണെന്ന് പറയാതെ തന്നെ.



ഒരു അധിക ഫയർവാൾ എന്ന നിലയിൽ, ഓരോ ഇടപാടിനും ഒരു പുതിയ കീ ജോഡി ഉപയോഗിക്കണം. മൾട്ടി-ഇൻപുട്ട് ഇടപാടുകളിൽ ചില ബന്ധപ്പെടുത്തൽ ഇപ്പോഴും ഒഴിവാക്കാനാവില്ല, അത് അവയുടെ ഇൻപുട്ടുകൾ ഒരേ ഉടമയുടെ ഉടമസ്ഥതയിലാണെന്ന് വെളിപ്പെടുത്തുന്നു. ഒരു കീയുടെ ഉടമ ആരെന്നുള്ള വിവരം പുറത്തായാൽ, എല്ലായ്പ്പോഴും ഒരേ കീ ജോഡി ആണ് ഉപയോഗിക്കുന്നതെങ്കിൽ അതേ ഉടമയുടെ മറ്റ് ഇടപാടുകൾ വെളിപ്പെടും എന്നതാണ് അപകടസാധ്യത.

11. കണക്കുകൂട്ടലുകൾ

സത്യസന്ധമായ ഒന്നിനെക്കാൾ വേഗത്തിൽ ഒരു ഇതര ചെയിൻ സൃഷ്ടിക്കാൻ ആക്രമണകാരി ശ്രമിക്കുന്ന സാഹചര്യം ഞങ്ങൾ പരിഗണിക്കുന്നു. ഇത് നിറവേറ്റിയാലും, നേർത്ത വായുവിൽ നിന്ന് മൂല്യം സൃഷ്ടിക്കുകയോ, ആക്രമണകാരിക്ക് ഒരിക്കലും ലഭിക്കാത്ത പണം എടുക്കുകയോ പോലുള്ള അനിയന്ത്രിതമായ മാറ്റങ്ങൾക്ക് ഇത് സിസ്റ്റം തുറന്നിടുകയില്ല. അസാധുവായ ഒരു ഇടപാട് പേയ്മെന്റായി നോഡുകൾ സ്വീകരിക്കാൻ പോകുന്നില്ല, മാത്രമല്ല സത്യസന്ധമായ നോഡുകൾ അവ അടങ്ങിയ ഒരു ബ്ലോക്ക് സ്വീകരിക്കില്ല. ആക്രമണകാരി അടുത്തിടെ ചെലവഴിച്ച പണം തിരിച്ചെടുക്കുന്നതിന് സ്വന്തം ഇടപാടുകളിൽ ഒന്ന് മാറ്റാൻ ശ്രമിക്കാം.

സത്യസന്ധമായ ചെയിനും ആക്രമണകാരിയുടെ ചെയിനും തമ്മിലുള്ള മൽസരത്തെ ബൈനോമിയൽ റാൻഡം വാക്ക് ആയി വിശേഷിപ്പിക്കാം. സത്യസന്ധമായ ചെയിൻ ഒരു ബ്ലോക്ക് നീട്ടുകയും അതിന്റെ ലീഡ് +1 വർദ്ധിപ്പിക്കുകയും ചെയ്യുന്നതാണ് വിജയ ഇവന്റ്, ആക്രമണകാരിയുടെ ചെയിൻ ഒരു ബ്ലോക്ക് നീട്ടുകയും വിടവ് -1 കുറയ്ക്കുകയും ചെയ്യുന്നതാണ് പരാജയ ഇവന്റ്.

ഇതിനകം പിന്നിലായ ഒരു ആക്രമണകാരി ഒപ്പം എത്താൻ സാധ്യത ഒരു ഗാംബ്ലേർസ് റൂയിൻ പ്രശ്നത്തിന് സമാനമാണ്. പരിധിയില്ലാത്ത ക്രെഡിറ്റുള്ള ഒരു ചൂതാട്ടക്കാരൻ ഒരു കമ്മിയിൽ പിന്നിൽ നിന്ന് ആരംഭിച്ച് ഒപ്പം എത്താൻ ശ്രമിക്കുന്നതിന് അനന്തമായ പരീക്ഷണങ്ങൾ നടത്തുന്നുവെന്ന് കരുതുക. അവൻ എപ്പോഴെങ്കിലും ഒപ്പം എത്തുന്ന സാധ്യത നമുക്ക് കണക്കാക്കാം, അല്ലെങ്കിൽ എപ്പോഴെങ്കിലും ഒപ്പം എത്തുമോ എന്ന് നോക്കാം [8]:

p = ഒരു സത്യസന്ധമായ നോഡ് അടുത്ത ബ്ലോക്ക് കണ്ടെത്താനുള്ള സാധ്യത

q = ആക്രമണകാരി അടുത്ത ബ്ലോക്ക് കണ്ടെത്താനുള്ള സാധ്യത

q_z = പിന്നിലുള്ള z ബ്ലോക്കുകളിൽ നിന്ന് ആക്രമണകാരി എപ്പോഴെങ്കിലും ഒപ്പം എത്താൻ സാധ്യത

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

p > q എന്ന ഞങ്ങളുടെ അനുമാനം അനുസരിച്ച്, ആക്രമണകാരിക്ക് ഒപ്പം എത്തേണ്ട ബ്ലോക്കുകളുടെ എണ്ണം കൂടുന്നതിനനുസരിച്ച് സാധ്യത ഗണ്യമായി കുറയുന്നു. പ്രതിബന്ധങ്ങൾ ഉള്ളപ്പോൾ നേരത്തെ തന്നെ ഭാഗ്യ മുൻതൂക്കം നേടാൻ ആയില്ലെങ്കിൽ, പിന്നിൽ ആകുമ്പോൾ അയാളുടെ സാധ്യതകൾ അപ്രത്യക്ഷമാകുന്നു

ഒരു പുതിയ ഇടപാടിന്റെ സ്വീകർത്താവ് ഇടപാട് മാറ്റാൻ അയച്ചയാൾക്ക് കഴിയില്ലെന്ന് ഉറപ്പാക്കുന്നതിന് മുമ്പ് എത്രത്തോളം കാത്തിരിക്കണമെന്ന് ഞങ്ങൾ ഇപ്പോൾ പരിഗണിക്കുന്നു. പണം അയക്കുന്ന ആൾ ഒരു ആക്രമണകാരിയാണെന്ന് ഞങ്ങൾ അനുമാനിക്കുന്നു, സ്വീകർത്താവ് തനിക്ക് കുറച്ച് സമയം പണം കിട്ടി വിശ്വസിക്കാൻ ആക്രമണകാരി ആഗ്രഹിക്കുന്നു, കുറച്ച് സമയം കഴിഞ്ഞാൽ അത് തിരികെ തനിക്കുതന്നെ അയക്കുന്നു. അത് സംഭവിക്കുമ്പോൾ സ്വീകർത്താവ് അലേർട്ട് ആകും, പക്ഷേ വളരെ വൈകി ആയിരിക്കും എന്ന് ആക്രമണകാരി പ്രതീക്ഷിക്കുന്നു.

സ്വീകർത്താവ് ഒരു പുതിയ കീ ജോഡി സൃഷ്ടിക്കുകയും സൈൻ ചെയ്യുന്നതിന് തൊട്ടുമുമ്പ് പബ്ലിക് കീ പണം അയക്കുന്ന ആൾക്ക് നൽകുകയും ചെയ്യുന്നു. അയയ്ക്കുന്നയാൾ സമയത്തിന് മുമ്പേ ഒരു ബ്ലോക്ക് ചെയിൻ തയ്യാറാക്കുകയും, അതിൽ തുടർച്ചയായി പ്രവർത്തിച്ചുകൊണ്ട് അയാൾക്ക് വളരെയധികം മുന്നോട്ട് പോകാനുള്ള ഭാഗ്യമുണ്ടാകുകയും തുടർന്ന് ആ നിമിഷം ഇടപാട് നടത്തുകയും ചെയ്യുന്നതിൽ നിന്ന് തടയുന്നു. ഇടപാട് അയച്ചുകഴിഞ്ഞാൽ, സത്യസന്ധനല്ലാത്ത പണം അയക്കുന്ന ആൾ തന്റെ ഇടപാടിന്റെ ഇതര പതിപ്പ് അടങ്ങിയ സമാന്തര ചെയിനിൽ രഹസ്യമായി പ്രവർത്തിക്കാൻ തുടങ്ങുന്നു.

ഇടപാട് ഒരു ബ്ലോക്കിലേക്ക് ചേർക്കുന്നതുവരെയും തുടർന്ന് z ബ്ലോക്കുകൾ ലിങ്കുചെയ്യുന്നതുവരെയും സ്വീകർത്താവ് കാത്തിരിക്കുന്നു. ആക്രമണകാരി കൈവരിച്ച പുരോഗതിയുടെ കൃത്യമായ അളവ് അയാൾക്കറിയില്ല, എന്നാൽ സത്യസന്ധമായ ബ്ലോക്കുകൾ ഒരു ബ്ലോക്കിന് ശരാശരി പ്രതീക്ഷിച്ച സമയമെടുത്തുവെന്ന് കരുതുകയാണെങ്കിൽ, ആക്രമണകാരിയുടെ പുരോഗതി ഒരു പോയിസ്സോൺ ഡിസ്ട്രിബ്യൂഷൻ ആയിരിക്കും, എക്സ്പെക്ടഡ് വാല്യൂ:

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

ആക്രമണകാരിക്ക് ഇപ്പോഴും ഒപ്പം എത്താനുള്ള സാധ്യത കണ്ടുപിടിക്കാൻ, അയാൾക്ക് നേടാൻ കഴിയുന്ന ഓരോ പുരോഗതിയുടെ അളവിന്റെയും പോയിസ്സോൺ ഡെൻസിറ്റിയെ ആ പോയിന്റിൽ നിന്ന് മുതൽ അയാൾ ഒപ്പം എത്താനുള്ള സാധ്യത വച്ച് ഗുണിക്കുന്നു:

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

ഡിസ്ട്രിബ്യൂഷനെ അനന്തമായി സംഗ്രഹിക്കുന്നത് ഒഴിവാക്കാൻ പുനർക്രമീകരിക്കുന്നു...

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

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;
}
```

z കൂടുമ്പോൾ എക്സ്പോണൻസിയായി സാധ്യത കുറയുന്നത് നമുക്ക് കാണാം.

```
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 0.1% ൽ താഴെ ആകുമ്പോൾ...

```
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. ഉപസംഹാരം

വിശ്വാസ്യതയെ ആശ്രയിക്കാതെ ഇലക്ട്രോണിക് ഇടപാടുകൾക്കായി ഞങ്ങൾ ഒരു സംവിധാനം നിർദ്ദേശിച്ചിട്ടുണ്ട്. ഡിജിറ്റൽ സിഗ്നേച്ചറുകളിൽ നിന്ന് നിർമ്മിച്ച നാണയങ്ങളുടെ പതിവ് ചട്ടക്കൂടിൽ

നിന്നാണ് ഞങ്ങൾ ആരംഭിച്ചത്, അത് ഉടമസ്ഥാവകാശത്തിന് ശക്തമായ നിയന്ത്രണം നൽകുന്നു, പക്ഷേ ഡബിൾ-സ്പെൻഡിങ് തടയുന്നതിനുള്ള മാർഗ്ഗമില്ലാതെ അപൂർണ്ണമാണ്. ഇത് പരിഹരിക്കുന്നതിന്, ഇടപാടുകളുടെ ഒരു പൊതുചരിത്രം റെക്കോർഡുചെയ്യുന്നതിന് പ്രൂഫ്-ഓഫ്-വർക്ക് ഉപയോഗിച്ച് ഒരു പിയർ-ടു-പിയർ നെറ്റ്വർക്ക് ഞങ്ങൾ നിർദ്ദേശിച്ചു, സത്യസന്ധമായ നോഡുകൾ സി.പി.യു. ശക്തിയുടെ ഭൂരിഭാഗവും നിയന്ത്രിക്കുകയാണെങ്കിൽ ആക്രമണകാരിക്ക് പൊതുചരിത്രം മാറ്റുന്നത് വേഗത്തിൽ അപ്രായോഗികമാകും. നെറ്റ്വർക്ക് അതിന്റെ ഘടനയില്ലാത്ത അസങ്കീർണ്ണതയിൽ ശക്തമാണ്. ചെറിയ ഏകോപനത്തോടെ നോഡുകൾ എല്ലാം ഒരേസമയം പ്രവർത്തിക്കുന്നു. സന്ദേശങ്ങൾ ഏതെങ്കിലും പ്രത്യേക സ്ഥലത്തേക്ക് വഴിതിരിച്ചുവിടാത്തതിനാൽ നോഡുകളെ തിരിച്ചറിയേണ്ട ആവശ്യമില്ല, മാത്രമല്ല മികച്ച ശ്രമത്തിന്റെ അടിസ്ഥാനത്തിൽ മാത്രമേ സന്ദേശങ്ങൾ കൈമാറു. നോഡുകൾക്ക് പോകാനും ഇഷ്ടാനുസരണം നെറ്റ്വർക്കിൽ വീണ്ടും ചേരാനും കഴിയും, അവ ഇല്ലാതിരുന്നപ്പോൾ എന്താണ് സംഭവിച്ചതെന്നതിന്റെ തെളിവായി പ്രൂഫ്-ഓഫ്-വർക്ക് ചെയിൻ സ്വീകരിക്കുന്നു. അവർ അവരുടെ സി.പി.യു. ശക്തി ഉപയോഗപെടുത്തി വോട്ടുചെയ്യുന്നു, സാധുതയുള്ള ബ്ലോക്കുകൾ വിപുലീകരിക്കുന്നതിൽ പ്രവർത്തിച്ചുകൊണ്ട് അവരുടെ സ്വീകാര്യത പ്രകടിപ്പിക്കുകയും പ്രവർത്തിക്കാൻ വിസമ്മതിച്ചുകൊണ്ട് അസാധുവായ ബ്ലോക്കുകൾ നിരസിക്കുകയും ചെയ്യുന്നു. ആവശ്യമായ ഏത് നിയമങ്ങളും പ്രോത്സാഹനങ്ങളും ഈ സമവായ സംവിധാനം ഉപയോഗിച്ച് നടപ്പിലാക്കാൻ കഴിയും.

പരാമർശങ്ങൾ

[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.