ቢትኮይን ፡ የአቻ ለ አቻ የኤሌክትሮኒክ ገንዘብ ሥርዓት

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

Amharic translation of Bitcoin.org/bitcoin.pdf by Ξ c r y p t o

ረቂቅ. ይህ ፍፁም የኤሌክትሮኒክ ገንዘብ ሙሉ ለሙሉ የአቻ ለ አቻ ስሪት ሲሆን ፡ ምንም አይነት የፋይናንስ ተቋም ሳያስፈልግ ከአንድ ወገን ወደ ሌላ ወገን በቀጥታ በበይነ መረብ ላይ ክፍያዎችን ለማድረግ ያስችላል ፡ ቢትኮይን ሰዎች ባንክ ሳያስፈልጋቸው በኢንተርኔት አማካኝነት ገንዘብ እንዲልኩ እና እንዲቀበሉ የሚያስችል ዲጂታል ገንዘብ ነው። ሁሉንም ግብይቶች የሚመዘግብ ትልቅ የዲጂታል መዝገብ የሆነውን ብሎክቼን (Blockchain) የሚባል ቴክኖሎጂ ይጠቀማል። ይህ ስርዓት ደህንነቱ የተጠበቀ ነው ምክንያቱም የክሪፕቶግራፊን አልጎሪዝም ስለሚጠቀም ማንም ለማጭበርበር ወይም ለመስረቅ በጣም አስቸጋሪ ያደርገዋል። ከ ቢትኮይን ቁልፍ ባህሪያቶች አንዱ ተደጋጋሚ የሚደረግን ድርብ ወጪን ወይም (Double spending) የመከላከል ችሎታው ሲሆን ይህም ማለት ተመሳሳዩን ቢትኮይን ከአንድ ጊዜ በላይ መጠቀም አያስችልም ። ቢትኮይን በዓለም አቀፍ ደረጃ ገንዘብን ለማስተላለፍ ፈጣን፣ ርካሽ እና አስተማማኝ መንገድ ለማቅረብ ያለመ ነው ።

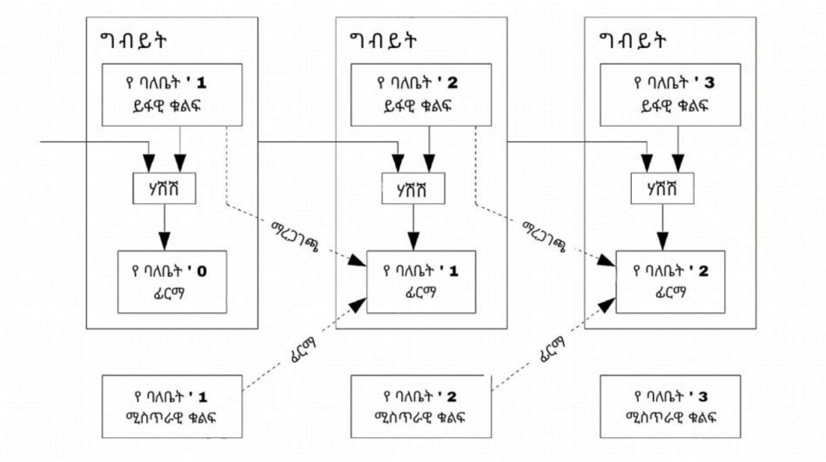
1. መግቢያ

አብዛኛው በበይነ መረብ የመስመር ላይ ያሉ የንግድ የክፍያ ስራዓቶች እንደ ባንኮች ባሉ የፋይናንስ ተቋማት ላይ ይተማመናል ። ይህ ስርዓት ለአብዛኛዎቹ ግብይቶች የሚሰራ ቢሆንም አንዳንድ ድክመቶች አሉት። ለምሳሌ ፡- ባንኮች አለመግባባቶችን መደራደር ስላለባቸው ግብይቶች ከተፈፀሙ በኋላ ሙሉ በሙሉ የማይመለሱ ሊሆኑ አይችሉም ። ይህም ወጪዎችን ይጨምራል እና አነስተኛ ግብይቶች ተግባራዊ አይሆኑም ፡ የግድ ነጋዴዎች ደንበኞቻቸውን ማመን አለባቸው የሄ ደሞ ወደ ማጭበርበር እና ከፍተኛ ወጪና ኪሳራ ያስከትላል ።

እነዚህን ችግሮች ለመፍታት ከእምነት ይልቅ በምስጠራዊ ማረጋገጫ ላይ የተመሰረተ የኤሌክትሮኒክ የክፍያ ስርዓት ያስፈልገናል። ይህ አሰራር ሁለት ወገኖች ታማኝ ሶስተኛ ወገን ሳያስፈልጋቸው በቀጥታ ግብይት እንዲፈጽሙ ያስችላቸዋል። ግብይቶች አስተማማኝ እና የማይመለሱ ይሆናሉ፣ ይህም ሻጮችን ከማጭበርበር ይጠብቃል ያድናል። አንዳንዶች ገዢዎችና ሻጮች ለተሻለ የእምነት ግብይት በ 3ተኛ ወገን በማስያዝ (Escrow Service) አገልግሎቶችን ይጠቀማሉ ። የእኛ መፍትሔ እያንዳንዱን የተፈፀሙ ግብይቶችን ከጊዜና ሰዓት ጋር ዲጂታል መዝገብ ላይ ማህተም በማድረግ ፡ ቅደም ተከተላቸውን በማረጋገጥ እና ድርብ ወጪን (Double spending) ለመከላከል የአቻ ለአቻ አውታረ መረብ በመጠቀም ችግሮችን እንፈታለን ። ሐቀኛ ተሳታፊዎች ከማንኛውም አጥቂዎች የበለጠ የኮምፒዩተር ኃይልን ወይም አቅምን እስከተቆጣጠሩ ድረስ ስርዓቱ ፤ ደህንነቱ የተጠበቀ ነው ።

2. ግብይት

የኤሌክትሮኒክ ዲጂታል ሳንቲምን እንደ ሰንሰለታዊ ዲጂታል ፊርማ መግለጽ እንችላለን ። እያንዳንዱ የ ዲጂታል ሳንቲም ባለቤት ያለውን ቢትኮይን ወደ ሌላ ወገን ሲያስተላልፍ ያለፈውን ግብይት እና የተቀባዩን የይፋ ቁልፍ በመጠቀም በዲጂታል መንገድ ይፈርማሉ ወይም የዲጂታል መዝገብ ላይ አሻራቸውን ያስቀምጣሉ ። ይህ ፊርማ ከ ቢትኮይን ግብይት ሰንሰለት ጋር ይተሳሰራል ። ከዚያም ተቀባዩ የባለቤትነት ሰንሰለትን ማረጋገጥ ይችላል ፡ ይህም ማለት ተቀባዩ ከዚ በፊት በየትኛው የቢትኮይን ባለቤት ተይዞ እንደነበር ማየት ማረጋገጥ ይችላል ።

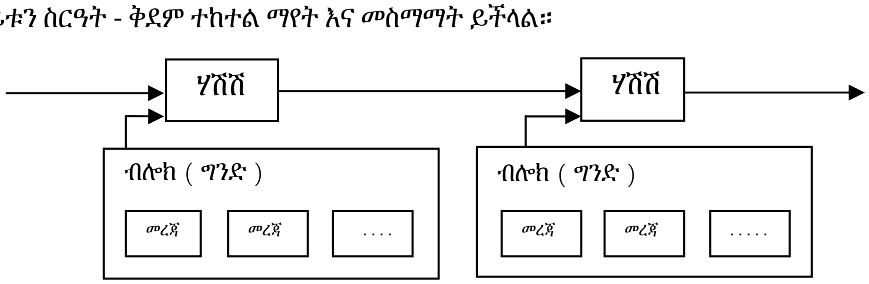


ችግሩ ተቀባዩ ፡ ላኪው አንድን ዲጂታል ገንዘብ ብቻ በመጠቀም ሁለትና ከዚያ በላይ ለግብይት ይጠቀም አይጠቀም እርግጠኛ መሆን አለመቻሉ ነው። የዚህ ችግር መፍትሄ ተብሎ የሚታመነው ማዕከላዊ ባለስልጣንን በማኖር ወይም አንድ ሚንት / ገንዘብ ሚመረትበት ቦታን ብቻ በመጠቀም ፡ ተደጋጋሚ ድርብ ወጪን ይቀርፋል ተብሎ ይታመናል ። በተዘዋዋሪ ከእያንዳንዱ ግብይት በኋላ፣ ቢትኮይን አዲስ ለማግኘት ወደ ሚንት ስርዓት መመለስ አለበት ፣ ይህም ድርብ ወጪ አለመደረጉን ያረጋግጣል። ሆኖም ይህ ስርዓቱ ከባንክ ጋር በሚመሳሰል መልኩ በአንድ ነገር ላይ ብቻ ጥገኛ ያደርገዋል።

ለዚይም የተሻለ መንገድ ያስፈልገናል፡፡ ላኪው ምንም የቀደመ ግብይቶችን እንዳልፈፀመ ተቀባዩ የሚያውቅበት መንገድ ያስፈልገናል። የመጀመሪያ የተፈፀመ ግብይት ወሳኙና ዋነኛው ነው ፤ ስለዚህ በኋላ ወይም ቀደም ሲል የነበረን ድርብ ወጪን ለማድረግ የተደረጉ ሙከራዎችን ችላ እንላለን። ያለ ሶስተኛ ወገን ሁለት ጊዜ ወጪ አለመኖሩን ለማረጋገጥ ሁሉም ግብይቶች በይፋ ለሁሉም መታወቅ ይኖርባቸዋል [1] ። ተሳታፊዎች በአንድ የግብይቶች መዝገብ ታሪክ ላይ የሚስማሙበት ስርዓት ያስፈልገናል። ተቀባዩ አብዛኛዎቹ ተሳታፊዎች ግብይቱን ለመጀመሪያ ጊዜ የተቀበሉት ለመሆኑ ማረጋገጫ ያስፈልገዋል።

1. የጊዜ ማህተም የሚቆጣጠር አገልጋይ

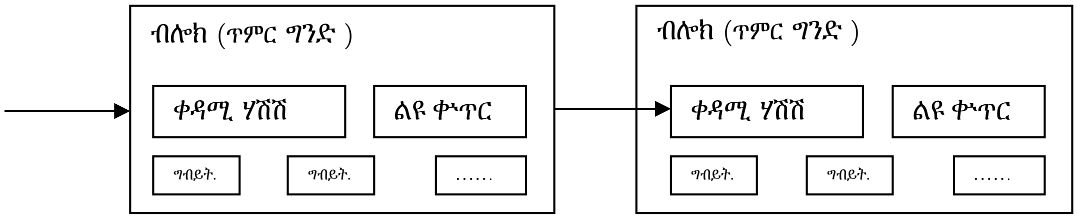
የጊዜ ማህተም አገልጋይ አሰራር በተለምዶ (Snapshot) ወይም በዲጂታል ቅጽበታዊ የገጽ ፎቶግራፍ) በማንሳት ልክ እንደ ጋዜጣ በሰፊው በዲጂታል መዝገብ ላይ በመታተም ይሰራል [2-5] ። ይህ የጊዜ ማህተም በዚያን ጊዜ ያሉ ነገሮችን ሁሉ እንደነበሩ እንደተመዘገቡ በዝርዝር ያሳያል ፤ያረጋግጣል ። እያንዳንዱ አዲስ ቅጽበታዊ የገጽ ፎቶግራፍ ቀዳሚውን ያካትታል ማለት ሁሉንም የቀደሙትን ቅጽበተ-ፎቶዎች ማረጋገጫን የሚያጠናክር ሰንሰለትን ይፈጥራል፡፡ የጊዜ ማህተም የሚቆጣጠር አገልጋይ ደህንነቱ የተጠበቀ ፤ ሊረጋገጥ የሚችል የክስተቶች ሰንሰለት ለመፍጠር ሃሽሽ (ግምገማዊ ተግባር/Hash) ይጠቀማል:: ይህም ሁሉም ሰው የግብይቱን ስርዓት - ቅደም ተከተል ማየት እና መስማማት ይችላል።



2. **ጥረት ላይ የተመሰረተ ማረጋገጫ** (Proof of Work)

የተበታተነ (የተከፋፈለ) የጊዜ ማህተም የሚቆጣጠር አገልጋይን በአቻ ለ አቻ መሰረት ለመተግበር ፡ ጥረት ላይ የተመሰረተን የማረጋገጫን ዘዴ ከ Adam Back's Hashcash ፡ [6] ፡ ጋር የሚመሳሰል የአሰራር ስርዓትን መጠቀም ይኖርብናል።
ጥረት ላይ የተመሰረተው ማረጋገጫ ልክ እንደ ልዩ ቁጥር ማግኘት መፈለግ ነው የዚህም ሂደት ስልተ ቀመር/ሃሺንግ ይባላል። ማለትም የነበረን ነገር ወይም አንድን ነገር በ [SHA -256] አልጎሪዝም በመጠቀም አስገብቶ ቀይሮ በአዲስ መልክ የማምጣት ሂደት ነው። ይህን ቁጥር ማግኘት ብዙ ሙከራዎችን ይጠይቃል ፡ ነገር ግን አንዴ ከተገኘ በኋላ ማንኛውም ሰው አንድ ጊዜ ውስጥ በማስገባት ትክክል መሆን አለመሆኑን በቀላሉ ማረጋገጥ ይችላል.።

በእኛ የጊዜ አውታረመረብ ማኅተም ውስጥ አዲስ ብሎክን ለመፍጠር ጥረት ላይ የተመሰረተ ማረጋገጫ የሚባለውን ዘዴ እንጠቀማለን። በዚህም አሰራር በተወሰነ የዜሮዎች ቁጥር እንዲጀምር የሚያደርገውን አንድ እስክናገኝ ድረስ በብሎክ ውስጥ ያለውን ቁጥር (nonce) ወይም ልዩ ቁጥርን መቀየርን ያካትታል። ይህንን ከባድ የጥረት ስራ ከጨረስን በኋላ እያንዳንዱን ብሎክ (ጥምር ግንድ) ዳግም ላይቀየር እንደ ብሎኬት ወደ ዲጂታል ሰንሰለቱ ውስጥ እንጨምራለን እንደረድራለን ።
አዳዲስ ብሎኮች ሲጨመሩ በፊት በነበረው ብሎክ በላይ በላዩ ነው ሚደረበው ፡ ስለዚህም ከዚ በፊት የነበረን ብሎክ መቀየር መለወጥ ማለት ከሱ በኋላ ለሚመጡት ብሎኮች ሁሉ እያንዳንዱን ስራውን መስራት ማለት ነው ይሄም በጣም ከባድና በጣም ጊዜ ሚፈጅ ነው ።



በይነመረብ ፕሮቶኮል አድራሻ (IP Address) ብዙ አይፒዎችን በመፍጠር የድምጽ ምርጫ ሊታለልና ሊጭበረበር ይችላል፡፡ ጥረት ላይ የተመሰረተው ማረጋገጫ ግን በኔትወርኩ ውስጥ ብዙ አብላጫ ውሳኔን በአንድ ሲፒዩ አንድ ድምጽ ለመወሰን ይረዳል ይጠቀማል። በጣም ረጅሙ የጥምር ብሎኮች ሰንሰለት የብዙሀኑን ውሳኔ ይወክላል ምክንያቱም በዚህ ሂደት ውስጥ ብዙ ሀይልና ጥረት ሚጠይቅ ነው። ሐቀኛ ተሳታፊዎች አብዛኛው የሲፒዩ ኃይል የሚቆጣጠሩ ከሆነ የዲጂታል ሰንሰለታቸው በፍጥነት ያድጋል እናም በጣም የታመነና የጠነከረ ይሆናል። ያለፈውን ብሎክ ለመቀየር አጥቂ ወይም ጠላፊ ለዛ ብሎክ እና ከሱ በኋላ ያሉትን ጥምር ብሎኮች ሁሉ እንደገና ከበፊቱ ብሎክ የበለጠ ሀይል ማውጣትና መስራት ይጠበቅበታል ፡፡ ጥረት ላይ የተመሰረተው ማረጋገጫ በጊዜ ሂደት አዳዲስ ብሎኮች ፈጥነውም ሆነ ዘግይተው በተፈጠሩ ቁጥር እራሱን በራሱ ያስተካክላል ፤ ይሄም ማለት በፍጥነት ብሎኮች ቢፈጠሩ ፈታኝ ያደርገዋል እንቆቅልሹን በዛው ልክ በዝግታ ብሎኮች ቢፈጠሩ ቀላል ያደርገዋል ። እንዲህ ብዙ ብሎኮች ሲጨመሩ ሲደራረቡ ይህ ይበልጥ ከባድና ማይናድ ይሆናል።

3. **ኔትዎርክ (አውታረ መረብ)**

ደረጃ በደረጃ ኔትወርኩን (አውታረ መረቡን) ለማካሄድ ሚከተሉት ናቸው :-

1) አዲስ ግብይቶች ለሁሉም በይነመረብ ኖዶች ይሰራጫሉ።
2) እያንዳንዱ የበይነመረብ ኖድ ማዕከል አዲስ ግብይቶችን በ ብሎክ ብሎክ አርጎ ይሰበስባል።
3) እያንዳንዱ የበይነመረብ ኖድ ማዕከል አስቸጋሪ የሆነውን እንቆቅልሽ ለማግኘት ይሠራል።
4) ልክ የበይነመረብ ኖዱ አስቸጋሪ የሆነውን እንቆቅልሽ ሲፈታ ብሎኩን ለሁሉም የበይነመረብ ኖዶች ያሰራጫል።
5) የበይነመረብ ኖድ ማዕከሎች ብሎኩን የሚቀበሉት በውስጡ ያሉት ሁሉም ግብይቶች ልክ ከሆኑና እስካሁን ከዚ በፊት ጥቅም ላይ ካልዋሉ ብቻ ነው።
6) የበይነመረብ ኖድ ማዕከሎች የሚቀጥለውን ብሎክ በመፍጠር ፤ በመጀመር አንድን ብሎክ እንደሚቀበሉ ያሳያሉ።
ተቀባይነት ያለው የብሎክ ሃሽሽ ተጠቅመው ከአዲሱ ብሎክ ጋር ያገናኙታል።

የበይነመረብ ኖድ ማዕከሎች ሁሌም ረጅሙን ሰንሰለት ወይም ብዙ ብሎክ ያለውን ትክክለኛና ተቀባይነት ያለው አርገው ይቆጥሩታል እናም በማራዘም መስራታቸውን ይቀጥላሉ። ሁለት የበይነመረብ ኖዶች የሚቀጥለውን ብሎክ የተለያዩ ስሪቶችን በተመሳሳይ ጊዜ ካሰራጩ ፡ አንዳንዶቹ ኖዶች የመጀመሪያው ይደርሳቿል አንዳንዶቹ ደሞ ሌላ ይደርሳቿል። በዚህ ሁኔታ በመጀመሪያ በተቀበሉት ላይ ይሠራሉ ነገር ግን ትልቅና ረጅም ከሆነ ሌላኛው ይይዙታል ። የሚቀጥለው ማረጋገጫ ሲከሰት ማሰሪያው ይቋረጣል እና አንድ ቅርንጫፍ ይረዝማል በሌላኛው ላይ ይሠሩ የነበሩት የአንጓዎች ቅርንጫፍ ወደ ረዥሙ ይቀየራል። አዲስ ጥረት ማስረጃ ሲገኝ አንድ የዲጂታል ሰንሰለቱ ረዘም ያለ ይሆናል። የበይነመረብ ኖድ ማዕከሎች በአጭር የዲጂታል ሰንሰለት ላይ የሚሠሩ የነበሩትም ወደ ረዘም ወደሚለው ይሄዳሉ ።

4. ማበረታቻ ክፍያ

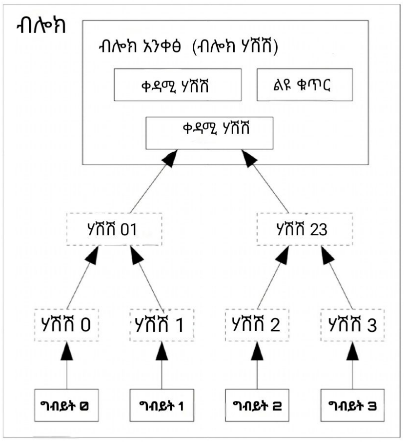
በብሎክ ውስጥ የመጀመሪያዋ የግብይት ሰነድ ልዩ ውል ነች ይቺም ለብሎክ ፈጣሪ አዲስ ዲጂታል ሳንቲምን ትፍጥራለች ፤ ይህም ማይነሮችን (የክሪፕቶግራፊክ ፈቺዎች) ለመደገፍ ያበረታታል እናም አዳዲስ ሳንቲሞችን ለማሰራጨት ይረዳል፣ እነርሱን ለማውጣት ማዕከላዊ ስልጣን የለም። የወርቅ ማዕድን ቆፋሪዎች ወርቅ ለማግኘት በሀብት እንደሚጠቀሙ ሁሉ ማይነሮችን (የክሪፕቶግራፊክ ፈቺዎች) አዳዲስ ዲጂታል ሳንቲሞችን ለመሥራት ሲፒዩ ፣ ጊዜና ፣ ኤሌክትሪክ ይጠቀማሉ።

በተጨማሪም የንግድ ልውውጡ ውጤት ላይ ከአስገቢው ያነሰ ከሆነ የልውውጥ ክፍያ ማግኘት ይችላሉ። በሆነ ጊዜ በቂ የሳንቲሞች ስርጭት ሙሉ ለሙሉ በገበያ ውስጥ ሲውል ለ ማይነሮችን (የክሪፕቶግራፊክ ፈቺዎች) ሲሰጥ የነበረው ዲጂታል ሳንቲሞች ይቀርና ወደ የግብይት ክፍያ ብቻ ሚቀየር ይሆናል ይህም ሲሆን የዋጋ ግሽበት ያስቀራል ።

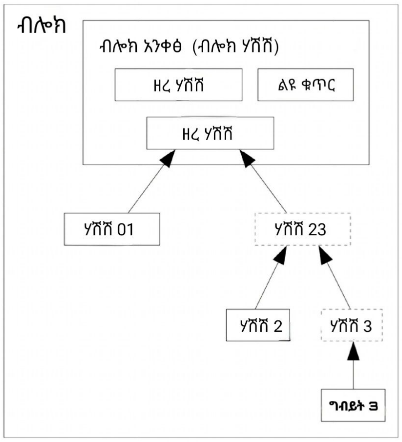
ይህ የማበረታቻ የክፍያ ሥነ-ስርዓት ማይነሮችን (የክሪፕቶግራፊክ ፈቺዎች) ሐቀኛ ሆነው እንዲቀጥሉ ይረዳል ይጠቅማል። አንድ ሰው የበለጠ ሲፒዩ ኃይል በመጠቀም ለማጭበርበር ቢሞክር ስርዓቱን ከማደናቀፍ ይልቅ ደንቡን በመከተል እና አዳዲስ የዲጂታል ሳንቲሞችን ማግኘት ትርፍን ይመርጣሉ ።

5. የዲስክ ቦታን (የመረጃ ቋትን) መልሶ መጠቀም

በአንድ የዲጂታል ሳንቲም ውስጥ አዲስ ልውውጥ ከተረጋገጠና ወደ ብሎክቼን ከተጨመረ በኋላ በጣም ቆየት ብለው ይተፈፀሙን ልውውጦች ለተሻለ የዲስክ ቦታ ማከማቻ ሲባል ሊወገዱ ወይም ሊጠፉ ይችላሉ። ይህንንም ለማፋጠን ከዲስክ ለበለጠ ማከማቻ ተብሎ፡አንድ ነገር ሲጠፋ የብሎኩ ልዩ መለያ ሳይለወጥ በቦታው ይቆያል። የዚህም ሂደት የሚደረገው የአዋቃሪ ቅርንጫፍን በመጠቀም ነው [7][2][5]። ይሄም ብዙ ግብይቶችን አንድ ላይ በ ልዩ ቀመር በማጣመር በብሎክ ውስጥ ሁሉንም እንደ አንድ ዘረ ሃሽሽ / ሀረግ አርጎ በ ብሎክ ውስጥ ማካተት ነው። አሮጌ የቅርንጫፎቹን ክፍሎች በመቁረጥ ቋጥኞችን እንዲያንሱ ያስችላል ፤ እናም የውስጠኛው ሃሽሽ መያዝ አያስፈልገም ።



ግብይቶች በአዋቃሪ ቅርንጫፍ ላይ ሲከተሩ
(Merkle Tree)

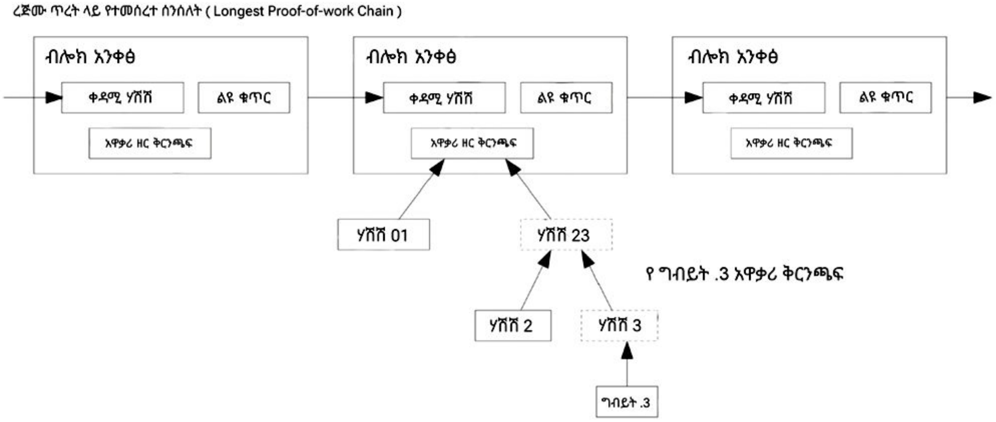


ከ ግብይት **0-2** ያለን የቆየ መረጃ ለ ዲስክ **(**የመረጃ ቋት**)**
ለመቆጠብ ከብሎክ ማጥፋት

ምንም ዓይነት የንግድ ልውውጥ የሌለበት የብሎክ አናት ውይም አንቀፅ 80 ባይት (80 bytes) ገደማ ይሆናል። እያንዳንዱ ብሎክ በየ 10 ደቂቃው ቢፋጠር ብለን ስናሰላ ፤ 80 ባይት * 6 * 24 * 365 = 4.2MB (ሜጋባይት) በየዓመቱ ይፈጠራል ። በአብዛኛው ከ2008 ዓ.ም እ.አ ወዲህ ኮምፒዩተሮች በራም (2GB RAM) ጀምሮ በገበያ ላይ ይሸጣሉ። የሞር ሕግ የአሁኑን እድገት በ 1.2GB በየዓመቱ ይተነብያል። ሚሞሪ/ የማከማቻ ቋት ምንም እንኳን ብዙ መረጃ በብሎክ ዋና አንቀፅ/ ስፍራ ላይ ብዙ ቦታ ቢይዝም ችግር መሆን የለበትም ።

6. ቀላል የክፍያ ማረጋገጫ

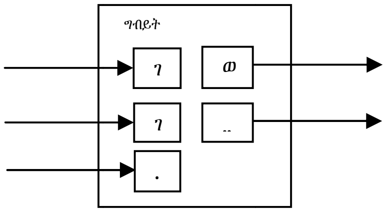
ሙሉ የበይነመረብ ኖድ (Full Node) በኮምፒውተራችን መተግበር ሳያስፈልግ ክፍያዎችን ፣ ግብይቶችን ማረጋገጥ ፤ ትክክል መሆናቸውን ማጣራት ይቻላል። አንድ የበይነመረብ ኖድ በኮምፒውተሩ ሚተገብር ሰው የብሎኩን ዋና አንቀፅ ቅጂ/ግልባጭ ብቻ መያዝ ያስፈልገዋል። በመቀጠል ማግኘት የሚችለውን እጅግ ረጅም የሆነ የማስረጃ-ጥረት ሰንሰለትን በጣም ረጅም ሰንሰለት እንዳለው እርግጠኛ እስኪሆን ድረስ በመረብ ውስጥ ያሉ ሌሎች ኮምፒውተሮችን በመጠየቅ እነዚህን ማግኘት ይችላል። በተጨማሪም የንግድ ልውውጡን ከተመዘገበበት ብሎክ ጋር የሚያያይዘው አዋቃሪ ቅርንጫፍ ያስፈልገዋል ። ምንም እንኳን የንግድ ልውውጡን እራሱ ማረጋገጥ ባይችልም ፤ አውታረ መረቡ እንደተቀበለው ማየት ይችላል። ከሱ በኋላ አዳዲስ ብሎኮች ሲጨመሩ አውታረ መረቡ መቀበሉን ይቀጥላል።



በመሆኑም ሐቀኛ ተሳታፊዎች የአውታረ መረቡን በይበልጥ እስከተቆጣጠሩት ድረስ በጣም አስተማማኝ ነው። ነገር ግን አውታረ መረቡ በጠላፊዎች ወይም አጥቂዎች በይበልጥ ከተቆጣጠሩት ለጥቃት ተጋላጭ ነው። የአውታረ መረብ ኖዶች የራሳቸውን ግብይት ማረጋገጥ አቅም ስላላቸው ፡ አጥቂው ቀለል ባለ ዘዴ/ፈጠራ ሊታለል ይችላል፤ ይዬም ጥቃት የሚፈፅመው ግለሰብ የአውታረ መረቡን በይበልጥ ለመቆጣጠር እስከቀጠለ ድረስ ለማጥቃት ይሞክራል። እንዲ አይነት ጥቃትን ለመከላከል አንድ ስልት ማምጣትን ይፈልጋል። ይሄም በበይነመረብ ኮምፒዩተር ኖዶች የሚመጣን የተሳሳቱ ብሎኮችና ሌላ ችግሮችን በማስጠንቀቂያ መልክ መቀበል ነው። ተጠቃሚውን ሙሉ የብሎኮች ሶፍትዌር በመጫን/ዳውንሎድ እንዲያረጉ በማነሳሳት ማናቸውንም ምልክት የተደረገባቸውን ወይም የተጠቆመባቸውን ችግሮች ለመፍታት ያስችላል። በተደጋጋሚ/በብዛት ግብይት ሚፈፅሙ የንግድ ድርጅቶች ወይም ግለሰቦች የተሻለ ዋስትናና የግብይት ፍጥነት ለማግኘት ሲሉ የራሳቸውን የኮምፒይተር ኖዶች በራሳቸው መተግበርን ይመርጡ ይሆናል።

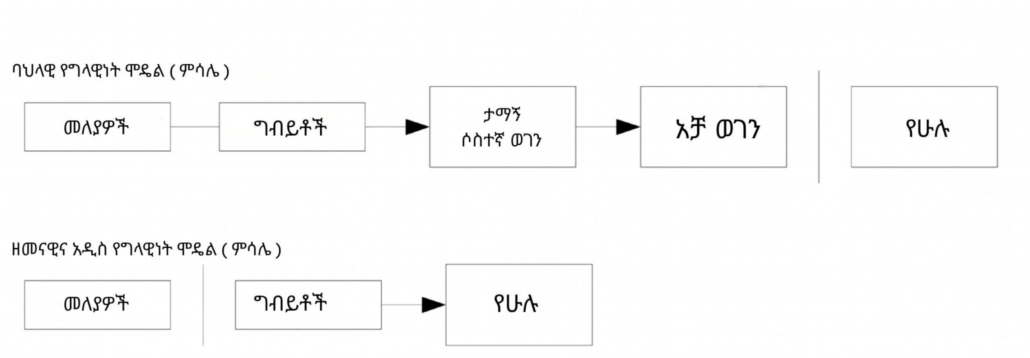
የውህደት እና የመከፋፈል እሴት

እያንዳንዱን የዲጂታል ሳንቲም አሃድ ለየብቻ መላክ ይቻላል ግን በጣም የተወሳሰበ ያደርግብናል። የንግድ ልውውጦች ንረት ሊደመርና ሊከፈል ይችላል ፡ የንግድ ልውውጥ አብዛኛውን ጊዜ አንድ ወይም ከዚያ በላይ አስመጪዎች (የገንዘብ ምንጮች/ገቢ) እና እስከ ሁለት የሚደርሱ ወጪዎች አሉት ይሄም አንዱ ለክፍያ ውጤቶቹ አንዱ ደግሞ ማንኛውም ወደ ላኪው ለመመለስ ይሆናል ።



7. ግላዊነት

ባህላዊው የባንክ ሞዴል ጉዳዩ የሚመለከታቸው ወገኖችና እምነት የሚጣልባቸው ሦስተኛ ሰዎች መረጃ በመገደብ የግላዊነት ደረጃን ያሳካዋል። ሁሉም የንግድ ልውውጦች በይፋ ይፋ መሆን አለባቸው ስለዚህ እኛ ምስጢር ማድረግ አንችልም : ይሁን እንጂ አሁንም ቢሆን የይፋ ወይም የህዝብ ቁልፎችን (እንደ ዲጂታል አድራሻ) ስማቸው እንዳይጠቀስ በማድረግ ግላዊነትን መጠበቅ እንችላለን። በዚህ መንገድ ሰዎች የንግድ ልውውጥ እንደተከናወነ ማየት ይችላሉ ፤ ነገር ግን ማን ግለሰብ ከማን እንደላከና እንደተቀበለ ማወቅ አይቻልም። ይህ ከአክሲዮን ሽያጭ ጋር ተመሳሳይነት አለው : የንግዱ ዝርዝር ይፋዊ/የህዝብ ነው ነገር ግን የነጋዴዎቹ ማንነት ግን አይኖርም።



እንደ ተጨማሪ ፋየርዎል ወይም ለበለጠ ደህንነት ለእያንዳንዱ ግብይት አዲስ ቁልፍ ወይም አድራሻዎችን በመጠቀም ከአንድ ባሌበትነት ብቻ ተያያዥነት እንዳይኖረው ያረጋል። አንዳንድ ግንኙነቶችን ማስወገድ የሚከብድ ነው ፤ ሌላ እዲስ ያልተጠቀምንበት ዋሌት/የዲጂታል የኪስ ቦርሳ ተጠቀምን ካልሆነ በቀር በድሮ ባለቤትነታችንን/ማንነታችን በተገለጠት ፣ በይፋ በሆነበት አድራሻችን ወደ ሌላ ስናስተላልፍም ሆነ ወጪ ስናረግ ፤ የቱ የማን እንደሆነ በቀደሙት የግብይት መዝገባችን ላይ ስለሚኖር ሙሉ ለሙሉ ድራሹን ማጥፋት ይከብዳል።

8. ስሌቶች

ተለዋጭ ሰንሰለት ለመፍጠር የሚሞክር አጥቂ ከሃቀኛዎቹ በበለጠ ፍጥነት ያለውን ሁኔታ እንመለከታለን ። ምንም እንኳን ይህ ቢፈፀም ስርዓቱን ወደ የዘፈቀደ ለውጦች አይመራውም : ለምሳሌ ከቀጭን አየር ውስጥ እሴት መፍጠር ወይም የአጥቂው ንብረት ያልሆነን ገንዘብ እንደ መውሰድ ማለት ነው። ይን ልክ ያልሆነ ግብይት እንደ ክፍያ አንቀበልም እና ሐቀኛ የኮምፒዩተር ኖዶች ይህን ፈጽሞ አይቀበሉም። እነሱን የያዘው አጥቂ መልሶ ለመውሰድ ከራሱ ግብይቶች አንዱን ብቻ ለመቀየር መሞከር ይችላል። በቅርቡ ያጠፋው ገንዘብ በታማኝ ሰንሰለት እና በአጥቂ ሰንሰለት መካከል ያለው ውድድር እንደ Binomial ሊገለጽ ይችላል። የሐቀኛ ሰንሰለት በአንድ ብሎክ እየተራዘመ በ+1 ይመራል ይጨምራል፤ እና የውድቀቱ ክስተት የአጥቂው ሰንሰለት በአንድ ብሎክ የተዘረጋ ሲሆን ይህም ክፍተት በ -1 ይቀንሳል። የአንድ አጥቂ ወይም ጠላፊ እጣ ፋንታ ትንሽ ጉድለት ወይም ክፍተትን የመያዝ እድሉ ከቁማርተኛ ጋር ተመሳሳይ ነው።

እንበልና አንድ ቁማርተኛ አስፈላጊውን ያህል ገንዘብ ሊበደር እንደሚችል አድርጋቹ አስቡት እናም ይህ ቁማርተኛ ገና ከጀምሩ ይበላል/ይከስራል ከዛም ያለገደብ ጨዋታውን በመጫወት እስከ ሚያሸንፍ ወይም የነበረውን እስኪያስመልስ ድረስ ይቀጥላል።

p = ይህ ሐቀኛው ተሳታፊ በአውታረ መረብ ውስጥ ቀጣዩን ብሎክ የማግኘት ዕድል ነው።
q = ይህ የጥቃት ፈፃሚው ወይም ጠላፊው ግለሰብ ቀጣዩን ብሎክ የማግኘት ዕድል ነው።
qz = ይህ የጥቃት ፈፃሚው ወይም ጠላፊው ግለሰብ ምንም እንኳን ከሀቀኛው ተሳታፊ በብሎክ ያነሰ አቅም ቢኖረውም መድረስ የሚችልበት ዕድል አለው።

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

የአጥቂው ኃይል (q) ከመረብ ኃይል (p) ያነሰ ከሆነ፣ ተጨማሪ ብሎኮች ሲጨመሩ አጥቂው የመያዝ ዕድሉ በፍጥነት ይቀንሳል። አጥቂው ቀደም ብሎ እድለኛ ካልሆነ የስኬት እድላቸው በጣም አነስተኛ ይሆናል። አንድ ሰው አዲስ ልውውጥ ሲቀበል : ላኪው ሊለውጠው እንደማይችል ለማረጋገጥ መጠበቅ ያስፈልጋል። ላኪው ሐቀኝነት የጎደለው ድርጊት ቢፈፅም የከፈሉት መስሎ እንዲታይ ለማድረግ ይሞክሩ ይሆናል ፤ ከዚያም በኋላ ላይ ይለውጡት ይሆናል። ተቀባዩ ያስተውላል ነገር ግን ላኪው በጣም ዘግይቶ እንደሚመጣ ተስፋ ያደርጋል። ይህንን ለመከላከል መቀበያው አዲስ ቁልፍ ጥንዶችን ይፈጥርና ከመፈረሙ በፊት ለላኪው ይፋዊ ቁልፍ ይሰጣል። ይህም ላኪው የሐሰት የብሎክ ሰንሰለቶችን አስቀድሞ ከማዘጋጀት ይቆጠበዋል። የንግድ ልውውጦቹ ከተላኩ በኋላ ሐቀኝነት የጎደለው ላኪ በስውር የሚሠራው በሌላ ዓይነት የንግድ ልውውጥ ሰንሰለት ላይ ነው። ተቀባዩ የንግድ ልውውጡ እስኪቆይ ድረስ ይጠብቃል እናም ከዚያ በኋላ ሌሎች በርካታ ብሎኮች ይጨመራሉ። አጥቂው ምን ያህል እድገት እንዳደረገ በትክክል አያውቁም ነገር ግን ሐቀኞች የተለመደውን ጊዜ ወስደዋል ብለው ያስባሉ።

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

አንድ አጥቂ አሁንም ሊያገኝ የሚችልበትን አጋጣሚ ለማወቅ ምን ያህል መሻሻል ሊያደርግ እንደሚችል እናሰላለን፤ ከዚያም ከዚያ ለመድረስ በሚችለው አጋጣሚ እናባዛለን።

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

ማለቂያ የሌላቸውን ተከታታይ ቁጥሮች ላለመጨመር ስንል ስሌቱን እንደገና እናስተካክለዋለን።

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

ወደ C ኮድ መቀየር...

```
#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;
}
```

ውጤቱን ስናሰላ በ (z) እየጨመረ ሲሄድ እድሉ በፍጥነት እንደሚቀንስ እናያለን.

```
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
```

የ (P) ዋጋን ለማግኘት ከ 0.1% ያነሰ ነው...

```
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
```

9. መደምደሚያ

በመተማመን ላይ የማይመካ የኤሌክትሮኒክ ልውውጥ ስርዓት ፈጥረናል። በዲጂታል ፊርማዎች የዲጂታል የሳንቲሞችን ባለቤትነት ለመቆጣጠር ያሳችለናል፤ ይህ ብቻ ድርብ ወጪን አይከላክልም ነገር ግን ድርብ ወጪን ለመከላከል የ ጥረት ላይ የተመሰረተን ማረጋገጫንና የአቻ ለአቻ አውታረ መረብን በመጠቀም እነዚህን ችግሮች እንፈታቸዋለን። ሀቀኛ የበይነመረብ ኖድ ወይም ኮምፒዩተር ሀይልን በብዛት እስተቆጣጠሩ ድረስ ለአጥቂው መዝገቡን ለመቀየር በጣም አስቸጋሪ ያደርገዋል። በአውታረ መረብ ውስጥ ቀላል እና ጠንካራ ኖዶች (ኮምፒዩተሮች) በብዙ ቅንጅት ሆነው አብረው ይሰራሉ ፤ መልዕክቶችም በአጠቃላይ ወደ አውታረ መረቡ ስለሚላኩ መለያ ማግኘት አያስፈልጋቸውም። የኮምፒዩተር ኖድ ተግባሪዎች በማንኛውም ጊዜ ከአውታረ መረብ ሊወጡ እና እንደገና ሊቀላቀሉ ይችላሉ። የኮምፒዩተር ኖድ ተግባሪዎች በሚሄዱበት ጊዜ የተፈጸመውን ነገር ለማሳየት የሚያስችል ማስረጃ ባለው የጥረት ማረጋገጫ ሰንሰለቱ ላይ ይተማመናሉ እናም በኮምፒዩተር ሀይላቸው ፣ ስልጣናቸው ድምጽን ለመስጠት ይጠቀሙበታል። ትክክለኛ የሆኑ ብሎኮችን በእነሱ ላይ በመስራት ፣ በማረጋገጥ እና ትክክል ያልሆኑትን ውድቅ በማድረግ ተቀባይነት ያላቸውን ብሎቶች ይቀበላሉ ያሰርፃሉ። ይህ ልዩ የስምምነት ሂደት ስርዓቱ እንዲሰራ የሚያስፈልጉትን ደንቦችና ማበረታቻዎች ያስፈጽማል።

ማጣቀሻዎች

[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.

የትርጉም ማስታወሻዎች

ይህ ትርጉም በከፍተኛ ጥንቃቄ የተዘጋጀ ቢሆንም በምንም መልኩ በሳቶሺ ናካሞቶ ከተፃፈው የእንግሊዝኛው ሰነድ **bitcoin.org/bitcoin.pdf** ጋር ፍጹም ምትክ ነው ማለት አይደለም ። ይህ ሰነድ በጥንቃቄ ጥቅም ላይ መዋል ይኖርበታል።

ይሄንንም በ አማርኛ የተተረጎመ ሰነድ በመጠቀም ለመላው ህዝብ በቋንቋው የበለጠ እንዲረዳው በመተርጎም አስተዋፆ እንድታደርጉ እንጠይቃለን ።

Nodes	በይነመረብ ኖድ
Block	ብሎክ (ጥምር ግንድ) / የዲጂታል ቋት
Nonce	ልዩ ቊጥር
Network	አውታረ መረብ
Internet	በይነ መረብ
Proof of work	ጥረት ላይ የተመሰረተ ማረጋገጫ
Snapshot	ቅጽበተ ፎቶ / የዲጂታል ቅጽበታዊ የገጽ ፎቶግራፍ
Merkle tree	አዋቃሪ ቅርንጫፍ
Merkle Root	ዘረ ሃረግ / አዋቃሪ ዘር ቅርንጫፍ
Block Header	ብሎክ አንቀፅ
Miners	ክሪፕቶግራፊክ ፈቺዎች
Hash	(ሃሽሽ) ስልተ ቀመር
Time Stamp	የጊዜ ማህተም