ብሎክቼይን

ለጀማሪ የአማርኛ አንባቢያን በሚመች መልኩ ተዘጋጅቶ የቀረበ

በናትናኤል ብሩክ

ማውጫ

01

ብሎክቼይን ምንድነው?

03

ብሎክቼይን እንዴት ነው የሚሰራው

06

ሚስጥራዊ ረቂቅ ሳጥን/Hash Function

08

የግብይት ገፆች ለውጥ

10

የ51% ጥቃት ምንድነው?

ብሎክቼይን ምንድነው?

እልም ያለ ጫካ ውስጥ የሚኖር ካልሆነ በቀር ከተማ ቀመስ የሆነን የህይወት መንገድ የሚከተል ግለሰብ በዚህ ባለንበት ወቅት ምንነቱን ባያውቅ እንኳን የቢትኮይንንና ብሎክቼይን ቴክኖሎጂን ስም ያልሰማ አለ ለማለት ይከብዳል። አሁን አሁን በተለይም ባደጉት አገሮች ከቴክኖሎጂ እና ፋይናንስ የተገኙ እመርታዎችን ሁሉ ያጨናነቀው ይኸው የብሎክቼይን ቴክኖሎጂ ነው። ይሁንና በዚች ሩጫ በበዛባት አለም ጊዜው ሳይኖርህ/ሽ ስለዚህ ጉዳይ ካልሰማህ/ሽ ይህ በጉዳዩ ምንነት ዙሪያ የሚያተኩር አጠር ያለ የማብራሪያ ፅሁፍ ላንተ/ቺ ነው። በተለይም ከትርጉሙ አንስቶ እስከ ትግበራው፤ ከምንነቱ አንስቶ እስከ ቴክኒካል ገለፃዎቹ ለሰዎች ለማስረዳት እና በቀላሉ እንዲገባቸው ለማድረግ እጅጉን ከባድ እንደሆነ በሚነገርለት በዚህ አዲስ የቴክኖሎጂ እመርታ ዙሪያ ቀላለ እና መሰረታዊ እውቀትን ለመገብየት ለሚፈልግ ሁነኛ መርጃ ፅሁፍ ነው ብዬ አምናለው። ይኸው ተግባር ቴክኖሎጂውን ላመጡት አመንጪዎች ባመጡበት የእንግሊዘኛ ቋንቋ ለማስረዳት ከከበደ በአማርኛ ሁሉም በሚገባው መልኩ ቅርፅ ለማስያዝ አስቸጋሪ ቢሆንብኝም እነሆ የሞከርኩትን ለህዝብ በነፃ አቅርቤያለው። መልካም ንባብ።

ብሎክቼይን ምንድነው ታዲያ?
ለምሳሌነት ያህል ብሩክታዊት የምትባል እህት አለህ እንበል። ከከተማ ውጪ የምትኖር ታናሽ እህትህ እንደሆንች እናስብ። አንድ ቀን ገንዘብ እጇ ላይ እንደጨረሰች እና የጤና እክልም ስላጋጠማት 10ሺህ ብር እንድትልክላት ትጠይቅሀለች። ታናሽ እህትህ ናትና እንደ ወንድም ልትደርስላትና ያለችህን ገንዘብ ለመላክም ብርህን ወደምታስቀምጥበት ባንክ ትሄዳለህ። በባንኩ ለሚያስተናግድህ የደንበኛ አገልግሎት መኮንንም ከአካውንትህ ላይ 10ሺህ ብር ወደብርኩታዊት አካውንት እንዲያስተላልፍ የወረቀት ማዘዣ ታቀርባለህ። የባንኩ ሰራተኛም በኮምፒዩተሩ ላይ የባንኩን የዳታቤዝ ስርዓት በመክፈት ባንተ ስም በተመዘገበው አካውንት ላይ ይላክልኝ ያልከው የገንዘብ መጠን መኖሩን ያረጋግጣል። በአካውንትህ ብር እንዳለ ካረጋገጠ በኋላም ከአንተ የገንዘብ መጠን ላይ በመቀነስ ወደ ብሩክታዊት አካውንት የተገለፀውን የብር መጠን ያስተላልፋል።

ለብሩክታዊት ብሩን እንዳስተላለፍክላት እና በአካውንቷ የጠየቀችህን 10ሺህ ብር እንደገባላት በስልክ ትነግራታለህ።

አሁን ከላይ ባስቀመጥኩት ምሳሌ ላይ የሆነውን ሁነት ንቃተ-ህሊናህን አተኩረህ በመስጠት እንመልከት። በዚህ የገንዘብ ዝውውር ላይ ምንም አይነት እውነተኛ የሚባል የጥሬ ገንዘብ [physical money] ዝውውር አልተካሄደም። ይልቅስ በአጭሩ ምንም አይነት የጥሬ ገንዘብ እንቅስቃሴ ሳያስፈልግ የባንክ ሰራተኛው በኮምፒዩተሩ ስክሪን ላይ በተመለከተው የባንኩ ዳታቤዝ[የመረጃ ማስቀመጫ ቋት] ላይ ቁጥሮችን ብቻ በማስገባት የገንዘቡን ባለቤትነት ከአንተ ወደብሩክታዊት ሊቀይረው ቻለ። ይህን የመረጃ ቋት ስርአት ግን አንተም ሆነ እህትህ ብሩክታዊት የማየትም ሆነ የመቆጣጠር ሲቀጥልም ሙሉ የሆነ የባለቤትነት መብትም ጭምር የላችሁም። ባይሆን አንተም ሆነ እህትህ በባንኩ ላይ እምነት በመጣል የገንዘብ ዝውውሩን እንደሚያደርግላችሁ በመተማመን ብራችሁን ለባንኩ አሳልፋችሁ መስጠታችሁ አንድ እውነት ሆኖ እናገኘዋለን። አንዱ የነባራዊው የባንክ ስርዓት ባህሪይም ነው። በእርግጥም በዚህ መሰል በሶስተኛ ወገን በሚደረግ የንብረት ማስቀመጥ እና ማስተላለፍ ስርዓት አለም መመራት ከጀመረች ዘመናትን አስቆጥራለች። ምናልባትም በዚህ ቅፅበት ይህንን የባንክ ስርዓት አካሄድ እንደችግር ለምን ሰዎች ያያታል ታዲያ የሚል ጥያቄ በጭንቅላታችሁ እንደሚመጣ እምነቴ ነው። ችግሩ ከባንክ ስርዓቱ ሳይሆን ለሰዎች ከሚሰጠው የፋይናንስ ስርዓት ነፃነት ጋር ቢያያዝ እንጂ ሌላ አይሆንም።

ይህንን ፅንሰ-ሀሳብ የበለጠ አጎልብቶ ለማስቀመጥ እንሞክር። በመጀመሪያ ያደረከው የገንዘብ ዝውውር የተደረገው በባንኩ የደንበኞች አገልግሎት መኮንን አማካኝነት በተደረገች አንዲት በኮምፒዩተር ላይ በተደረገች የቁጥር ምዝገባ ለውጥ ብቻ መሆኑን ማስታወስ ተገቢ ነው። ይህ ደግሞ የስርአቱን ታማኝነት ጥያቄ ውስጥ ለመጣል አንድ ብቻ ግለሰብ ወይም ድርጅት የሚፈልግ አካሄድ ያደርገዋል።

ለምሳሌ ከዚህ ጋር ተያይዞ ሊነሱ ከሚችሉ ጥያቄዎች መካከል፡

- የአንተን እና የእህትን የገንዘብ መጠን መረጃ የያዘው መዝገብ በተለያዩ ምክንያቶች የመጥፋት አደጋ ቢደርስበትስ? [ለምሳሌ እጅጉን የረቀቁ የሀኪንግ ጠበብቶች የባንኩን የውሂብ ስርአተ-መረብ ውድመት ቢያደርሱበትስ?]
- አካውንቱን የሚያስተዳድረው የደንበኞች አገልግሎት መኮንን 10,000 ብሎ ማስገባት የነበረበትን በስህተት 15,000 ብር ብሎ ቢመዘግበውስ?
- ይህንን ተግባር አውቆ ቢያደርግውስ?

ታዲያ ይህንን በባንኩ የመረጃ ቋት ውስጥ የሚገኝን የውሂብ ስብስብ እንዴት ሙሉ ለሙሉ የተጠበቀ እና ከአደጋ የነፃ ማድረግ ይቻለናል?
አሁን አንዲት ቅፅበት ውሰዱና ሁለት አጫጭር ጥያቄዎችን ልጠይቃችሁ።
1. የገንዘብ ዝውውር ሲባል ከስረመሰረቱ ምንድነው?
2. የራሳችንን ገንዘብ ወደሌላ ለማስተላለፍ ግዴታ እንደባንክ ያሉ ሶስተኛ ወገኖች ሁሌም ያስፈልጉናል ማለት ነው ወይስ ያለእነዚህ ባንኮች፤ የሬሚት አገልግሎት ሰጪዎች እና ሶስተኛ ወገኖች የራሳችንን መዝገብ በመያዝ እና ጣልቃ ገብነታቸው ሳያስፈልገን በራሳችን ማሳካት ይቻለን ይሆን?

መልሳችሁ አዎ! ይቻላል፤ የሚቻለውም በብሎክቼይን ቴክኖሎጂ አማካኝነት ነው ከሆነ በእርግጥም ትክክለኛውን ምላሽ ገምታችኋል። ከላይ ላነሳሁት ጥያቄ መልሱ በእርግጥም የብሎክቼይን ቴክኖሎጂ የሚል ነው። አጠር ባለ መልኩም ብሎክቼይን ማለት ሰዎች በዚህ መስክ የሚፈልጉትን የተዓማኒነት ስራ እና የባንኩን የምዝገባ ስርዓት ምንም አይነት የሶስተኛ ወገን ጣልቃ ገብነት ሳያስፈልግ ማድረግ እንዲቻል የሚያደርግ የግብይት መመዝገቢያ ስርዓት ማለት ነው።

በዚህ ደረጃ ላይ ቴክኒካል ሁኔታዎቹን ወደማስረዳት ከገባሁ ነገሩን የበለጠ ግራ አጋቢ ስለማደርገው በመጀመሪያ ሶስት በዚህ ሁነት ላይ ልትረዱ የሚገባቸውን ነጥቦች አንስቼ ልለፍ፡

1.ብሎክቼይን ማለት የተለያዩ ግብይቶችን በዲጂታል መንገድ የምናደርግበት እና የልውውጦቹንም መረጃ የምንመዘግብበት የመዝገብ አያያዝ ስርዓት ነው፡፡

2.ገንዘብን ለማስተላለፍ ምንም አይነት ባንክም ሆነ ሌላ ሶስተኛ ወገን አያስፈግም፡፡

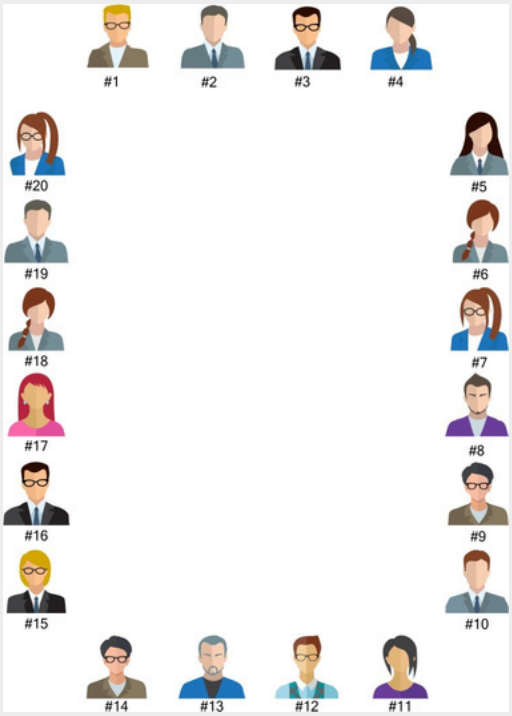
3.በማእከላዊ ባንክ በሚታተሙ ገንዘቦች ፋንታ ዲጂታል መገበያያ ከረንሲዎችን እና ንብረቶችን እንደግብአት የሚጠቀም ይሆናል፡፡

እነዚህ ሶስት ነጥቦች ግራ አጋብተዋችኋል? ወደዋናው የብሎክቼይን ምንነት እየተንደረደርን ስለሆነ ግር እንዳይላችሁ፡፡ ብቻ ብሎክቼይን በእነዚህ ከላይ በተገለፁት ሶስት ሁነቶች ላይ የተመሰረተ ቴክኖሎጂ እንደሆነ በልቦናችሁ ያዙ፡፡

ብሎክቼይን ታዲያ እንዴት ነው የሚሰራው?

የብሎክቼይን ስርአት በስራ ላይ እንዲተገበር ቢያንስ ሶስት ግለሰቦች በመጀመሪያ ከዚህ የሶስተኛ ወገን ጥገኝነት በመውጣት በብሎክቼይን ስርአቱ ለመሳተፍ ያስፈልጋሉ፡፡ የስርአቱን አሰራር ሂደት በይበልጥ ለመረዳት በምሳሌ እንደግፈው እና በምሳሌያችንም 20 ግለሰቦችን እንውሰድ፡፡ እነዚህ 20 ግለሰቦች የራሳቸውን የሆነ በብሎክቼይን ቴክኖሎጂ የሚዘወር የፋይናንስ ስርአት ለመመስረት የተስማሙ ግለሰቦች እንደሆኑ እናስብ፡፡

በዚህ መዋቅር ውስጥ የብሎክቼይን ስርአቱ የሚፈልገው ሁሉም የመረቡ አባላት ስለእያንዳንዱ አባል የአካውንት መረጃ በእጁ ላይ የሚገኝ ይሆናል፡፡ ይሁንና ማንነታቸው እና ግላዊ መረጃዎቻቸውን ግን ፈፅሞ አንዳቸው የሌላኛውን የማያውቁት ይሆናል ማለት ነው፡፡



ምሳሌያችንን እንቀጥል እና በዚህ በምሳሌነት በመሰረትነው የብሎክቼይን የፋይናንስ መረብ ውስጥ የሚያስፈለጉትን ሁነቶች ደረጃ በደረጃ በቅደም ተከተከል እንመለከት።

1.በመጀመሪያ ሁሉም የመረቡ አባላት የየራሳቸው የሆነና ለመረጃ አያያዝ ይጠቅማቸው ዘንድም እያንዳንዱ አባል የራሱ የሆነ ባዶ ማህደር እንደሚኖረው እናስብ። በዚህም :-
-እያንዳንዱ የቡድኑ አባል ባዶ የሆነ ማህደር ይኖረዋል።
-እያንዳንዱ ግለሰብ ግብይቶችን ከቡድኑ አባላት ጋር በሚያደርግበት ቅፅበት ሁሉ የግብይቱ መረጃ የተከተበበትን አዲስ ገፅ የሚመዘገብ ሲሆን ይህንንም ገፅ በሂደት ባዘጋጀው የመረጃ ማስቀመጫ ማህደር የሚያስቀምጥ ይሆናል።
-እነዚህ የተመዘገቡ ገፆች ተሰብስበው የምዝገባ ስርአቱን እያንዳንዱን የገንዘብ ስርአት መዝግበው የሚያስቀምጥ ማህደርን ይፈጥራሉ ማለት ነው።

2. የግብይት አፈፃፀም : እያንዳንዱ የመረቡ አባላት በመረቡ ውስጥ የሚደረጉ ግብይቶችን ከመጀመሪያው አንስተው የሚመዘግቡ ይሆናል። የሚመዘግቡትም ከላይ ያስፈልጋቸዋል ተብሎ በተገለፀው እና በሚኖራቸው የመረጃ መመዝገቢያ ባዶ ወረቀት አማካኝነት እንደሆነ አስቡት። ለምሳሌ በምስሉ ላይ ከተመለከቱት የቡድኑ አባላት መካከል በተራ ቁጥር 3 ላይ ያለው ግለሰብ በተራ ቁጥር 9 ለሚገኘው ወዳጁ 1000 ብር መላክ ፈለገ እንበል። ይህንን የገንዘብ ልውውጥ/ግብይት ለማድረግ ቁጥር 3 ሁሉም አባላት በሚመለከተበት ሁነት “ለተራ ቁጥር 9 1000 ብር መላክ እፈልጋለው።” የሚል መረጃን ያስተላልፋል።

በዚህ ቅፅበት እያናዳንዱ የመረቡ አባላት ገንዘቡን መላክ የሚፈልገው ቁጥር 3 በአካውንቱ በቂ ገንዘብ መኖሩን ያረጋግጣሉ። ይህንንም የሚያደርጉት ከላይ ከጅምሩ ለመግለፅ እንደተሞከረው እያንዳንዱ የመረቡ አባላት የእያንዳንዱን አባላት የአካውንት መረጃ በእጃቸው ማግኘት ስለሚችሉ መሆኑ ልብ ይሏል። ተራ ቁጥር 3 እንደገለፀው ለተራ ቁጥር 9 የሚያስተላልፈው በቂ የሆነ ገንዘብ እንዳለው ሲያረጋግጡም እያንዳንዱ የመረቡ አባላት ባዘጋጁት የመረጃ መመዝገቢያ ወረቀት ላይ በማስፈር ግብይቱን ያረጋግጣሉ።

September 20, 2022 - 11:11 AM

ቁጥር 3 ....ቁጥር 9 ብር. 1,000 /-

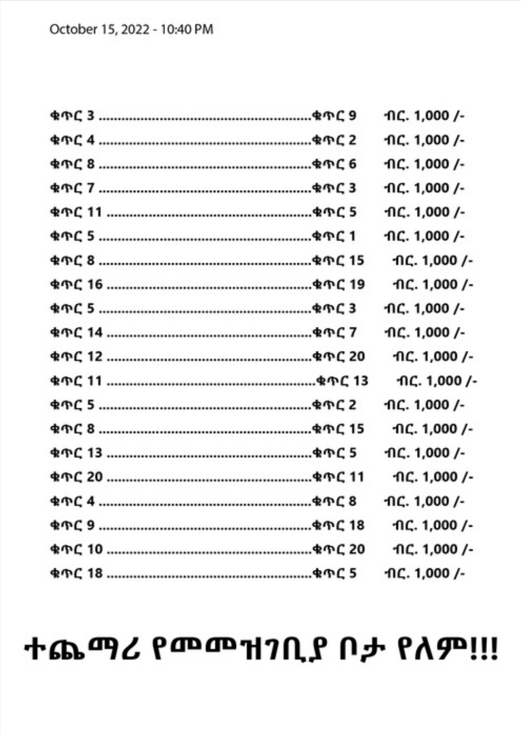
ማስታወሻ : እያንዳንዱ የመረቡ አባላት የተረደረጉ እያንዳንዱ ግብይቶችን በመመዝገቢያ ገፆቻቸው እና ማህደራቸው ውስጥ መዝግበው የሚያስቀምጡ ይሆናል።

ተጨማሪ ማስታወሻ : በምሳሌነት እያየነው ባለው በዚህ ሁነት ላይ ሀያዎቹ አባላት በብሎክቼይን የግብይት ምዝገባ ስርአት “Nodes” ብለን የምንጠራቸውን አካላት የሚወክሉ ይሆናል። በዚህም ግብይቱ/የገንዘብ ዝውውሩ በተሳካ ሁኔታ መፈፀሙን ማረጋገጥ ይቻላል ማለት ነው።

3.የግብይቶች ቁጥር መጨመር :
አንዴ ይህ የብሎክቼይን የግብይት መረብ በስራ ላይ ከዋለ በኋላ በመረቡ ውስጥ የሚገኙ ግለሰቦች እርስ በእርሳቸው የሚያስተላልፉት የገንዘብ ዝውውር እንደሚጨምር ከግምት በማስገባት ምሳሌያችንን እንቀጥል። በዚህም እያንዳንዱ ግለሰብ ገንዘብን ለሌላ የመረቡ አባል ለማስተላልፍ በሚፈልግበት ጊዜ ከላይ የገለፅነውን አካሄድ የሚከተል ይሆናል ማለት ነው። ስለሆነም ሁሉም አባል ለመዘዋወር ብቁ የሆኑ የገንዘብ ዝውውሮችን ሁሉ እያረጋገጡ መራጃውን በሚይዙበት ገፅ ላይ የተረጋገጡ ግብይቶችን የሚመዘግቡ ይሆናል ማለት ነው። ይህ ሁነት እያንዳንዱ ግለሰብ መረጃውን በሚከትብበት የመመዝገቢያ ገፅ ላይ ቦታ እስከሚያጣ ድረስ መመዝገቡን የሚቀጥል ይሆናል።

ላነሳነው ምሳሌ እያንዳንዱ አባል በአንድ የመረጃ መሰብሰቢያ ወረቀት/ገፅ ላይ መመዝገብ የሚችለው 20 የገንዘብ ዝውውሮችን ነው ብለን እንውሰድ። በዚህ ምክንያትም እያንዳንዱ አባል 20 በመረቡ ውስጥ 20 ግብይቶችን/ የገንዘብ ዝውውሮችን መዝግበው ሲጨርሱ ለመመዝገቢያነት የሚጠቀሙበት ገፅ የሚሞላ ይሆናል ማለት ነው።

አሁን ተጨማሪ ግብይቶችን ለመመዝገብ የሚያስችል ተጨማሪ ቦታ ስለማይኖረንም የሞላውን የተረጋገጠ የግብይት/ የገንዘብ ዝውውር መረጃን የያዘ ገፅ መጀመሪያ ባዘጋጀነው የመረጃ መሰብሰቢያ ማህደር እናስቀምጣልን።
የግርጌ ማስታወሻ : ለአረዳድ ምቹ ይሆን ዘንድ እና ለምሳሌነት ይቀል ዘንድ በዚህ ምሳሌ ላይ የኢትዮጵያን ብር እንደመገበያያ ገንዘብ እንውሰድ እንጂ ከላይ ማስታወስ ከሚኖሩብን ሶስት ወሳኝ ነጥቦች ውስጥ እንደተገለፀው በብሎክቼይን የግብይት ምዝገባ ስርአት ውስጥ ጥቅም ላይ የሚውሉት እንደቢትኮይን እና ኢቲሪየም የመሳሰሉ በስነ-መሰውር[cryptography] ጥበብ የሚዘወሩ እና የሚሰሩ ክሪፕቶከረሲዎች[ምናባዊ መገበያያዎች] መሆናቸው ግዴታ መሆኑ ልብ ይሏል። ይህም በብሎክቼይን የቴክኒካል ገለፃዎች ላይ በዚሁ ፅሁፍ የመጨረሻ ክፍሎች ከነምክንያቱ ማብራሪያ የሚሰጠው ጉዳይ ይሆናል።


October 15, 2022 - 10:40 PM

ቁጥር 3	ቁጥር 9	ብር. 1,000 /-
ቁጥር 4	ቁጥር 2	ብር. 1,000 /-
ቁጥር 8	ቁጥር 6	ብር. 1,000 /-
ቁጥር 7	ቁጥር 3	ብር. 1,000 /-
ቁጥር 11	ቁጥር 5	ብር. 1,000 /-
ቁጥር 5	ቁጥር 1	ብር. 1,000 /-
ቁጥር 8	ቁጥር 15	ብር. 1,000 /-
ቁጥር 16	ቁጥር 19	ብር. 1,000 /-
ቁጥር 5	ቁጥር 3	ብር. 1,000 /-
ቁጥር 14	ቁጥር 7	ብር. 1,000 /-
ቁጥር 12	ቁጥር 20	ብር. 1,000 /-
ቁጥር 11	ቁጥር 13	ብር. 1,000 /-
ቁጥር 5	ቁጥር 2	ብር. 1,000 /-
ቁጥር 8	ቁጥር 15	ብር. 1,000 /-
ቁጥር 13	ቁጥር 5	ብር. 1,000 /-
ቁጥር 20	ቁጥር 11	ብር. 1,000 /-
ቁጥር 4	ቁጥር 8	ብር. 1,000 /-
ቁጥር 9	ቁጥር 18	ብር. 1,000 /-
ቁጥር 10	ቁጥር 20	ብር. 1,000 /-
ቁጥር 18	ቁጥር 5	ብር. 1,000 /-

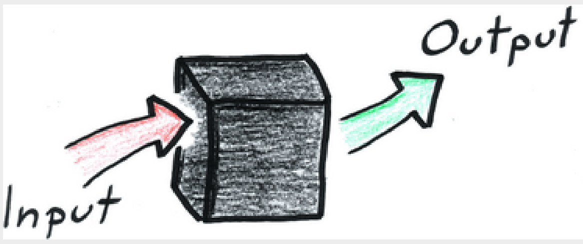
ተጨማሪ የመመዝገቢያ ቦታ የለም!!!

4.በምዝገባው ቦታ የሞላብንን ገፅ ደህንነቱ በተጠበቀ መልኩ ማስቀመጥ :
እዚህኛው የግብይቱ ደረጃ ላይ ስንደርስ አንድ አዲስ ነገር ላስተዋውቃችሁ። በብሎክቼይኑ መረብ ውስጥ ያሉ ሁሉም አባላት ይህንን እየተስማሙ ሁሉንም በመሀላቸው የተደረጉ ግብይቶች የፈፀሙባቸውን ገፅ በምንም ሁኔት እንዳይቀየር እና የመረጃ ስህተቶችን እንዳያመጣ ቆልፎ የሚያስቀምጥላቸው ሁሉም የሚስማሙበትን ልዩ መቆለፊያ ቁልፍ የሚያዘጋጁ ይሆናል። በዚህም ማንም ግለሰብ የተመዘገቡ መረጃዎችን ወደኋላ በመሄድ እንዳይለውጥ[ለምሳሌ መረጃው በእጁ እስካለ ድረስ ከዚህ በፊት የላከውን እና ከአካውንቱ ውጪ የሆነውን ገንዘብ መልሶ በራሱ ስም እንዳይመዘግብ ወዘተ] ሁሉም አባላት በሚስማሙበት ሁነት በየራሳቸው እጅ በሚገኘውና በዚሁ ቁልፍ ተቆለፎ የሚቀመጡትን ገፆች በሚያጠራቅሙበት ማህደራቸው መረጃውን የሚያስቀምጡት ይሆናል ማለት ነው።
ማስታወሻ : በዚህ ምሳሌ የተገለፀውን ሁነት በእውነተኛ የብሎክቼይን ትግበራ “ማይን” ማድረግ በማለት የሚጠራ ሲሆን ለአረዳድ ቀላል እና ምቹ ይሆንልም ዘንድ በዚህ ፅሁፍ ላይ ሁነቱን “መቆለፍ/locking” ብለን የምንጠራው ይሆናል።

ይህ ቁልፍ ታዲያ ምንድነው ጥቅሙ የሚል ጥያቄ ወደጭንቅላታችሁ ከመጣ መልሱ በዚህ ቅፅበት በመቆለፍ የምናለፈው የግብይቱ ሂደት በነባራዊው አለም በባንኮች ወይም ሶስተኛ ወገኖች አማካኝነት የሚፈፀመውን የደህንነት ጥበቃ ለማግኘት የሚረዳን ዋናው መሰረታዊ የቴክኖሎጂው ክፍል ነው የሚል ይሆናል።

ታዲያ መዝግበን የሞሉብንን ገፆች እንዴት አድርገን ነው መቆለፍ የምንችለው?
እንዴት ነው ገፁን መቆለፍ የሚቻለን የሚለውን ጥያቄ ከመመለሳችን በፊት አንድ መሰረታዊ የሆነ ነጥብ አለ፤ እንዴት ነው ይህ የአቆላለፍ ሁነት የሚሰራው? የሚለውን ጥያቄ መልስ ማግኘት በጉዳዩ ላይ ያለንን አረዳድ ይበልጡን የሚያቀለው ይሆናል።

ሚስጥራዊው ረቂቅ ሳጥን
እስቲ የሆነ የረቀቀ ሚስጥራዊ ሳጥን አላችሁ ብላችሁ አስቡት። ወደዚህ ሳጥን የሆነ አንዳች ነገርን በምታስገቡበት ቅፅበት ሳጥኑ ያስገባችሁለትን ነገር በቁጥር እና ፊደላት መልክ ተርጉሞ የሚያስቀምጥ የረቀቀ ሳጥን ነው ብለን እናስብ።



የግርጌ ማስታወሻ : በዚህ ምሳሌ ላይ እንደሚስጥራዊው ሳጥን የምንወስደው በነባራዊው የብሎክቼይን ስርአት ውስጥ “ሀሽ ፈንክሽን/Hash Function” ብለን የምንጠራውን ሁነት ሲሆን ለአረዳድ ቀላል ይሆን ዘንድም አጠራራችንን ሚስጥራዊ ሳጥን በሚል ስያሜ እናስቀጥል።

በዚህም መሰረት በዚህ ረቂቅ ሳጥናችን ውስጥ ለምሳሌ 6 ቁጥርን ስንከትለት ሳጥኑ ይህንን ያስገባንለትን መረጃ ሚስጥራዊ በሆነ ኮድ የሚሰጠን ይሆናል። በዚህም ለ6 ቁጥር የሚያወጣልን አዲስ አይነት ኮድ “vgfhrt3” የሚል ነው እንበል። በእርግጥ እንደስሙ የዚህን ረቂቅ ሳጥን ስራ በአግባቡ የሚረዳ ማንም ሊኖር አይቻለውም፤ ተያይዞም የዚህን ሳጥን የመጨረሻ መልስ ወደነበረበት እንመልሰው ቢባል

መመለስ የሚቻል አይሆንም። ይህም ማለት ሳጥኑ እንደመልስ የሰጠንን ኮድ በማየት ወደሳጥኑ የገባውን ቁጥር ማንም በምንም ሁነት ማወቅ አይቻለውም ማለት ይሆናል። ይሁንና በማናቸውም ጊዜ 6 ቁጥርን ወደ ሳጥኑ በምናስገባበት ወቅት ሳጥኑ በሁሉም ሁነቶች የሚሰጠን የተቀየረ ኮድ ከላይ ያገኘነውን “vgfhrt3” የሚል ይሆናል ማለት ነው።
ማስታወሻ ፡ ወደዚህ ሳጥን/hash function/ የምናስገባው መረጃ የፈለገ ጊዜያት ተደጋግሞ ቢገባለትም ለአንድ ለተሰጠው የመረጃ አይነት ሳጥኑ ሁሌም አንድ አይነት ኮድን የሚያመነጭ ይሆናል። በምሳሌያችን እንደማሳያ እንደሚታየውም 6 ቁጥርን ምንም ያህል ጊዜ ደጋግመን ብናስገባለት የሚሰጠን ሚስጥራዊ ኮድ ሁልጊዜም “vgfhrt3” የሚል ይሆናል።

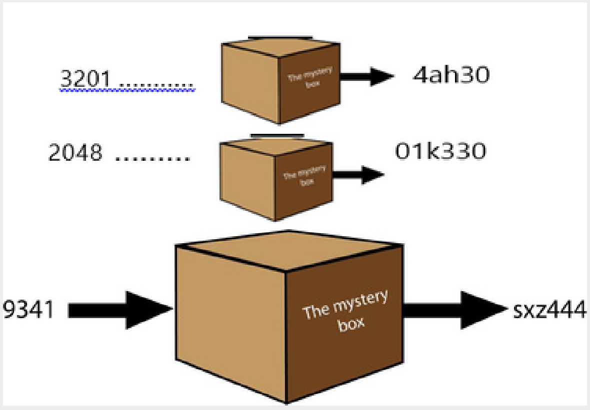
መመለስ የሚቻል አይሆንም። ይህም ማለት ሳጥኑ እንደመልስ የሰጠንን ኮድ በማየት ወደሳጥኑ የገባውን ቁጥር ማንም በምንም ሁነት ማወቅ አይቻለውም ማለት ይሆናል። ይሁንና በማናቸውም ጊዜ 6 ቁጥርን ወደ ሳጥኑ በምናስገባበት ወቅት ሳጥኑ በሁሉም ሁነቶች የሚሰጠን የተቀየረ ኮድ ከላይ ያገኘነውን “vgfhrt3” የሚል ይሆናል ማለት ነው።

ማስታወሻ ፡ ወደዚህ ሳጥን/hash function/ የምናስገባው መረጃ የፈለገ ጊዜያት ተደጋግሞ ቢገባለትም ለአንድ ለተሰጠው የመረጃ አይነት ሳጥኑ ሁሌም አንድ አይነት ኮድን የሚያመነጭ ይሆናል። በምሳሌያችን እንደማሳያ እንደሚታየውም 6 ቁጥርን ምንም ያህል ጊዜ ደጋግመን ብናስገባለት የሚሰጠን ሚስጥራዊ ኮድ ሁልጊዜም “vgfhrt3” የሚል ይሆናል።

አሁን አንድ ጥያቄ ልጠይቃችሁ። በዚህ ሚስጥራዊ ረቂቅ ሳጥን ምን አይነት ቁጥር ብናስገባ በተከታታይ ሶስት ዜሮዎች የሚጀምሩ እንደ 0003e, 000df, 000yu, 000xmd... የመሳሰሉ ኮዶችን ማግኘት ይቻለናል። የተወሰነ ጊዜ ወስዳችሁ መልሱን አስቡበት እና እንቀጥል።

አዎ በእርግጥም ጊዜያችሁን ወስዳችሁ መልሱን አስባችሁበት መልስ ነው የምትሉትን ኮድ ካመጣችሁ ተሳስታችኋል። ይልቅስ ከላይ ለመግለፅ እንደተሞከረው ሳጥኑ የሰጠንን የመጨረሻ መልስ/output/ በማየት ከቶውንም መጀመሪያ ወደሳጥኑ ያስገባነውን መርጃ/input/ ማወቅ ከቶውንም አይቻለንም። ስለዚህ ታዲያ ለዚህ ጥያቄ ምላሹን እንዴት ማግኘት ይቻለን ይሆን?

ለዚህ ጥያቄ መልስ ለመስጠት የተለያዩ መንገዶች ቢኖሩም የመጀመሪያው እና ቀጥተኛው ምናልባትም ግን እጅግ አድካሚውና ፈታኙ ሁነት ወደሳጥኑ ሊገቡ የሚችሉ እያንዳንዳቸውን ቁጥሮች ከመጀመሪያ አንስቶ እያስገቡ መሞከር ነው። በዚህ አካሄድ ምናልባትም እድለኞች ከሆንን አንድ ሺህ ሙከራዎችን ካደረግን በኋላ በሶስት ተከታታይ ዜሮ ቁጥሮች የሚጀምር ኮድ እናገኝ ይሆናል። በዚህም ያስገባነው ቁጥር ሁሌም በሳጥኑ ውስጥ በሚከተትበት ወቅት እንደውጤት የሚወጣው ተመሳሳይ ምላሽ/output/ እስከሆነ ድረስ ከዚያ በኋላ በሶስት ዜሮዎች የሚጀምር ወደሳጥኑ የሚገባ መረጃ በምንፈልግበት ወቅት ይኸው ስናስገባው ሶስት ተከታታይ ዜሮዎችን በመስጠቱ ሂደት የተሳካልን ቁጥር ከግምት እንድናስገባ ሊረዳን ይችላል። ይሁንና ግን በዚህ መንገድ ይህንን ማወቅ ይቻላል ማለት የመጨረሻው የሳጥኑ ውጤት ተሰቶን በመጀመሪያ እንደመረጃ የተሰጠውን መረጃ ማኝየት ግን አሁንም ከባድ መሆኑ እንዳለ ነው።



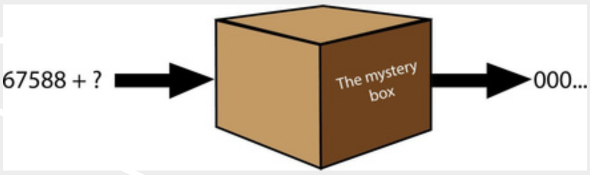
በእርግጥም አንድ በረቂቁ ሳጥን አማካኝነት የተገኘን ሚስጥራዊ ኮድ በማየት መጀመሪያ ወደሳጥኑ የገባውን ዳታ ለማወቅ እጅጉን በጣም ከባድ ይሁን እንጂ አንድ የተሰጠን ቁጥር የምንፈልገውን አይነት ኮድ እንደሚያወጣ እና እንደማያወጣ ለማወቅ እጅጉን ቀላል ነው በቀላሉ ያንን በሳጥኑ ውስጥ ሲገባ ምን አይነት ኮድ እንደሚያወጣለት የምንፈልገውን ዳታ ወደሳጥኑ ማስገባት ብቻውን በቂ ነው። ከዚያ ሚስጥራዊው ሳጥን በራሱ ኮድ በመስጠት ተፈላጊውን መረጃ/output/ የሚሰጠን ይሆናል። እዚህ ጋር ማስታወስ ካሉብን ዋና ነጥቦች መካከል እንደሳጥኑ በምሳሌያችን ላይ የወሰድነው በነባራዊው የብሎክቼይን እውነታ ሀሽ ፈንክሽን/hash function/ ብለን የምንጠራው ሚስጥራዊ ቀመር ሁለት ባህሪያት እንዳሉት ነው።

- አንድም የአንድን በሳጥኑ/ሀሽ ፈንክሽኑ/ አማካኝነት እንደ መልስ ያገኘነውን የመጨረሻ ውጤት በማየት ወደሳጥኑ /hash function/ የገባውን የውሂብ/ዳታ/ ምንነት ማወቅ እጅግ በጣም ከባድ መሆኑ ሲሆን:
- በሁለተኛነት ደግሞ አንድ ወደሳጥኑ የምናስገባው ውሂብ/ዳታ ካለን የመጨረሻ ከሳጥኑ የሚወጣውን ሚስጥራዊ ኮድ ማወቅ ደግሞ እጅጉን ቀላል መሆኑን ነው።

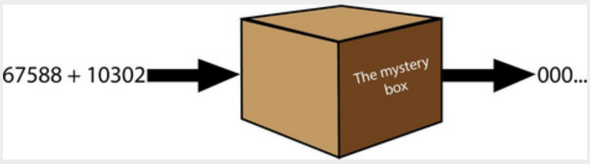
ታዲያ ይህንን ሚስጥራዊ ረቂቅ ሳጥን ተጠቅመን ግብይታችንን የፈፀምንበትን እና ሁሉም የተስማማበትን የመመዝገቢያ ገፅ እንዴት ደህንነቱ በተጠበቀ መልኩ ቆልፈን ልናስቀምጠው ይቻለናል?

ይህንን መልስ ለመመለስ አሁንም መላምታዊ ሁነትን እንደምሳሌ እናንሳ።

ሁለት ከሚስጥራዊ ሳጥን የተለዩ ሳጥኖች አሏችሁ እንበል። የመጀመሪያው ሳጥን 67558 የሚለውን ቁጥር በውስጡ የያዘ ነው። በመቀጠል እዚሁ ጋር አንድ ጥያቄ ላንሳ፡ ስንት ቁጥር በዚህ ሳጥን ውስጥ ከሚገኘው ቁጥር ጋር ብንደምረው እና በሚስጥራዊ ሳጥን ውስጥ ብናስገባው ነው በሶስት ተከታታይ ዜሮዎች የሚጀምር ኮድን ረቂቁ ሳጥን ሊሰጠን የሚችለው?

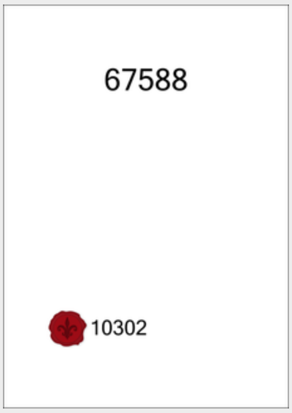


ከዚህ ጋር ተመሳሳይ የሆነ ጥያቄ ከላይ የጠየኳችሁ በመሆኑ መልሱ ያዳግታችኋል የሚል ፍራቻ የለኝም። በዚህም ልክ እንደመጀመሪያው ሁነት በዚህም ሁነት አንድ ከረቂቁ ሳጥን የወጣን ኮድ ካወቅን የገባውን መረጃ/input/ ለማወቅ ያለን የመጀመሪያ እድል የመሳካት እድሉ እጅግ አነስተኛ የሆነ እና አድካሚው ቁጥሮችን እየከተቱ መሞከር የሚለው መንገድ ይሆናል።አሁንም እድለኛ ሆንን እንበልና ከአንድ ሺህ ሙከራዎች በኋላ 10302 የሚለውን ቁጥር እንደሙከራ ስናስገባ እና ከላይ በምሳሌያችን አለን ብለን ባሰብነው የመጀመሪያ ሳጥን ያለንን 67558 ስንደምረው የሚሰጠንን ቁጥር[67558+10302=77854] ወደሚስጥራዊው ሳጥን በምናስገባበት ወቅት የተጠየቅነውን በሶስት ተከታታይ ዜሮዎች የሚጀምር ኮድ ሳጥኑ አመነጨልን እንበል።



በዚህ አጋጣሚ ታዲያ መልሱን ለማግኘታችን ቁልፍ ሚና የተጫወተው 10302 የተሰኘ ቁጥር አብሮት ለሚደመረው ቁጥር [67558] እንደ መቆለፊያነት የሚያገለግል ይሆናል ማለት ነው።

አሁን 67558 የሚለውን ቁጥር የያዘ የመመዝገቢያ ገፅ አስቡ። ይህንን ገፅ ለመቆለፍ 10302 የሚል ቁጥር እንደ ተደራቢ መቆለፊያ መኖሩ በቂያችን ይሆናል ማለት ነው። 10302 የሚለው ቁጥር በየትኛውም አጋጣሚ ከዚህ ቁጥር ጋር በአንድ ገፅ በሚገናኝበት ወቅት ገፁ የሚቆለፍ ይሆናል ማለት ነው።

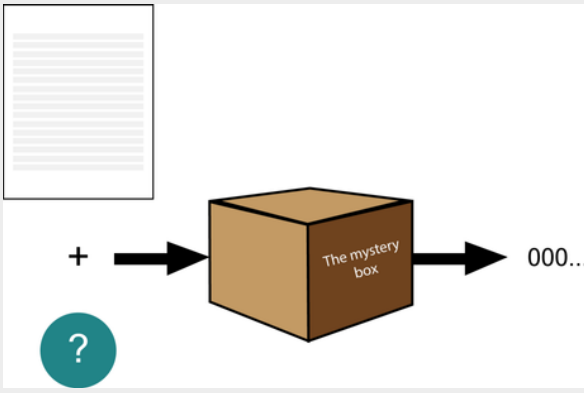


ማስታወሻ : ይህ በምሳሌያችን ላይ ለመቆለፊያነት ጥቅም ላይ የዋለው ቁጥር በብሎክቼይን ውስጥ “proof of work” ብለን የምንጠራው አካል ሲሆን ይህም ይህ ሚስጥራዊ ቁጥር የመረጃውን ገፅ በመቆለፍ ሂደት የተደረጉ ጥረቶች ስለመኖራቸው ማመሳከሪያ ይሆናል ማለት ነው። ለጊዜው ከላይ እያደረግን እንደመጣነው ለአረዳድ ቀላል እና ምቹ ይሆን ዘንድ ይህን ሁነት የመቆለፍ ሂደት እንደሆነ ማሰባችንን እንቀጥላለን።

በዚህም በዚያ የመረቡ አባላት ከትበው ባስቀመጡት ውሂብ/ዳታ ላይ ለውጥ አለመደረጉን ለማረጋገጥ በአጭሩ በገፁ ላይ የተገለፀውን መረጃ እንደአዲስ ከተገኘው የመቆለፊያ ቁጥር ጋር በመደመር ለሚስጥራዊው ረቂቅ ሳጥን ስናስገባለት በሚሰጠን ምላሽ ማወቅ ይቻላል። በዚህም በሚስጥራዊው ሳጥን የሚመጣልን ምላሽ በሶስት ዜሮዎችን የሚጀምርን ኮድ የሚሰጠን ከሆነ በዚያ ገፅ ላይ ያለው መረጃ እንዳለተቀየረ ማረጋገጫ ይሆነናል ማለት ነው።

ከላይ በምሳሌ እንደታየው ግን ይህ የመቆፊያ ቁጥር በገፁ ላይ ካለው መረጃ ጋር ተደምሮ ወደሳጥኑ በሚገባበት ወቅት የሚሰጠው ሚስጥራዊ ኮድ በሶስት ተከታታይ ዜሮዎችይ የሚጀምር ካልሆነ መረጃ በተመዘገበበት ገፅ ላይ የተደረገ ለውጥ እንዳለ ማሳያ ስለሚሆን ይህን መረጃ የያዘው የመረጃ መያዣ ወረቀት ውድቅ የሚደረግ ይሆናል ማለት ነው። በዚህ ሂደትም እያንዳንዱ ገፅ መመዝገቢያ ቦታ በጨረሰ ልክ በዚህ የሚስጥራዊ ሳጥን/hash function/ አማካኝነት ገፆቹን በመቆለፍ እና ባዘጋጀነው የመረጃ ወረቀቶች መሰብሰቢያ ማህደር ውስጥ እያስገባን ወደቀጣይ ግብይቶች የምንቀጥል ይሆናል ማለት ነው።

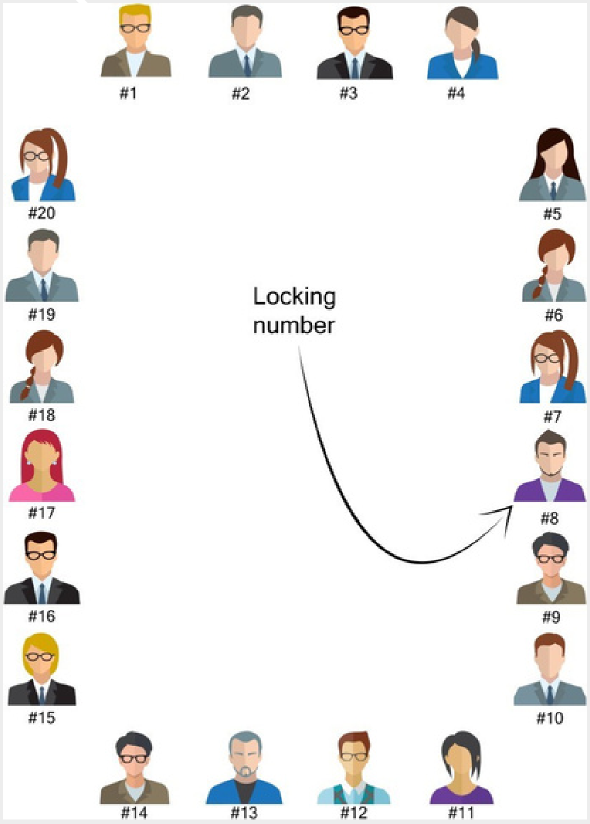
የግብይት ልውውጥ የመዘገብንበትን ገፅ እንዴት መቆየር:
እዚህ ነጥብ ላይ በእጃችን እንደመረጃ ካለን የገንዘብ ልውውጥ/transaction/ ላይ ስንደምረው እና በሚስጥራዊ ሳጥኑ ውስጥ ስናስገባው ተከታታይ ዜሮዎች ያሉትን ኮድ/output/ የሚሰጠንን ቁጥር ማወቅ ይኖርብናል።



ማስታወሻ : በዚህ ምሳሌ ላይ ሚስጥራዊ ሳጥኑ የሚሰጠንን ኮድ/output/ ለአረዳድ ምቹ ይሆን ዘንድ በሶስት ተከታታይ ዜሮዎች የሚጀምር አደረግነው እንጂ በእርግጥም በትክክለኛው የብሎክቼይን ስርአት ውስጥ የሚኖሩ የሀሽ ፈንክሽኖች ከዚህ በላቀ ሁኔታ የተወሳሰቡ እና ረጃጅምም ጭምር መሆናቸውን ማስታወስ ግድ ነው።

በዚህም ሁሉም አባላት መዝግበው ያስቀመጡት አንድ አይነት የመዝገብ ገፅ በሂሳባዊ ስሌት በተገኘው በዚህ አዲስ ቁጥር አማካኝነት ሊቆለፍ ይችላል ማለት ነው። በመሆኑም በመረቡ ውስጥ የሚገኝ ማንኛውም ግለሰብ በሁሉም እጅ ላይ ያለውን እውነተኛ የገንዘብ ልውውጥ መረጃ ቢቀይር እንኳን በሂሳባዊ ስሌት የተገኘውን ይህንን አዲስ ቁጥር በመከተት እና ሚስጥራዊ ሳጥኑ የሚሰጠውን የመጨረሻ ስሌት/output/ በማየት መለወጥ ወይም አለመለወጡን ማረጋገጥ ይቻላል ማለት ነው።

በምሳሌያችን መጀመሪያ ላይ እንደተገለፀው ከሆነ በፈጠርነው የግብይት መረብ ውስጥ አባላት 20 ግብይቶችን ከመዘገቡ በኋላ የመመዝገቢያ ቦታው/ገፁ እንደሚያልቅ አንስተናል። ይህ የመጨረሻው ግብይት በተደረገበት ቅፅበትም አባላቱ ገፁን ደህንነቱ በተጠበቀ መልኩ ለማስቀመጥ የሚረዳቸውን ሚስጥራዊ ኮድ የሚለዩ ይሆናል።



ይህንን የመቆለፊያ ቁጥር ሁሉም በብሎክቼይን መረቡ ውስጥ የሚገኙ አባላት በኮምፒዩተሮቻቸው አማካኝነት መፈለግ የሚችሉ ሲሆን ከሁሉም መጀመሪያ ትክክለኛውን ስሌት ያገኘው ግለሰብ ለሁሉም የመረቡ አባላት ትክክለኛውን ምላሽ እንዳገኘ ያሳውቃል። ይህ የስሌት ምላሽ የደረሳቸው የመረቡ አባላት በበኩላቸው ትክክል ነው የተባለውን ስሌት በሚስጥራዊው ሳጥን ውስጥ በመክተት ትክክለኛነቱን የሚያረጋግጡ ይሆናል። ትክክለኛውን ምላሽ በስሌቱ መሰረት የሚያገኙ ከሆነ ሁሉም በስሌቱ በመስማማት በጉፁ ላይ የዚህን ስሌት ምላሽ በማያያዝ ወደገፁ ማስቀመጫ ማህደራቸው በማስቀመጥ ሌላ አዲስ መመፅገቢያ ገፅ ላይ ግብይቶችን መመዝገብ የሚጀምሩ ይሆናል ማለት ነው።

በዚህ አጋጣሚ ግን ከመረቡ አባላት መካከል አንዱ ግለሰብ ትክክለኛ የሚባለው ኮድ/output/ ከሚስጥራዊው ሳጥን ውስጥ በትክክለኛው መንገድ ባይወጣለትስ?
ለምሳሌ ያህል በቁጥር 17 ላይ የተመለከተችው ግለሰብ ሌሎቹ የመረቡ አባላት በትክክል የመጣላቸው የሂሳብ ስሌት ባይመጣላትስ? ለዚህ አጋጣሚ መንስ ሊሆኑ ከሚችሉት ዋና ዋና ምክንያቶች መካከል፡

1. **በተሳካ ሁኔታ ስሌቱን አግኝቼዋለው ያለው አባል የገለፀውን የስሌት ቁጥር በተሳሳተ ሁነት አስገብታለች፤**
2. **የተገለፀውን የግብይት/transaction/ ውሂብ/ዳታ በተሳሳተ ሁነት አስገብታለች፤ አሊያም**
3. **ራሷን ወይም ሌላ በመረቡ ውስጥ ያለን አባል ለመጥቀም ሆን ብላ ለማሳሳት ሙከራ አድርጋለች።**

መንስኤው የተለያየ ሊሆን መቻሉ እንዳለ ሆኖ በቁጥር 17 ላይ የምትገኘው የመረቡ አባል በእንዲህ ያለው ሁነት ያላት ምርጫ አንድ እና አንድ ብቻ ነው። ይህም የራሷን ግብይት የተመዘገበበት ገፅ በመጣል ሌሎቹ አባላት የተስማሙበትን ትክክለኛውን የግብይት መረጃ የያዘ ገፅ ኮፒ መያዝ ነው። በዚህም ከሌላ አባል ያገኘችውን ይህን የተመዘገበ ግብይት በወረቀት ማስቀምጫ ምህደሯ ውስጥ የምታስቀምጥ ይሆናል ማለት ነው። ቁጥር 17 ይህንን ሁነት ባትከተልና ትክክለኛውን መረጃ የያዘውን ገፅ በማህደሯ የማታስቀምጥ ከሆነ ግን ያንን እስከምታደርግ ድረስ ምንም አይነት ግብይቶችን በመረቡ ውስጥ መፈፀም አይቻላትም ማለት ነው።

ማስታወሻ ፡ በዚህ ሁነት እንደትክክለኛ የመቆለፊያ ቁጥር የሚወሰደው ቁጥር በመረቡ ውስጥ ከሚገኙ አባላት መካከል አብላጫው አባላት የተስማሙበት ቁጥር መሆኑም በመሰረታዊነት ልብ ሊባል የሚገባ ነጥብ ነው።

ታዲያ አብዛኛው ሰው ጊዜውን በመሰዋት፤ ትልልቅ የኮምፒዩተር አውታሮችን እና ትልቅ የሚባል የኤልክትሪክ ሀይልን በመጠቀም ሌላ ሰው ሊያደርገው የሚችለውን ይህንን ስሌት የማወቂያ አድካሚ መንገድ እንዴት ለማድረግ ወሰነ?

መልሱ ቀላል ነው። ይህንን ስሌት በመፈፀም በግብይት ስርአቱ ደህንነት ላይ አሻራቸውን ያሳረፉ አባላት ሁሉ ይህንን በማድረጋቸው ሽልማት ይኖራቸዋል። ይህንን ስሌት ለመፈፀም ሁሉም በመረቡ ውስጥ በአባልነት ያሉ ግለሰቦች ሁሉ ማድረግ የሚችሉ ሲሆን ይህንን ስሌት ከሁሉም ቀድሞ በትክክለኛነት ያገኘው አካል ብቻ ተከፋይ ላደረገው አስተዋፅኦ ተከፋይ ይሆናል።

ከምሳሌያችን በመነሳት ለምሳሌ ቁጥር 6 ለመጀመሪያው ገፅ መቆለፊያነት የሚያገለግለውን ስሌት አገኘ እንበል። በሂደቱም ከብሎክቼይን ሲስተሙ/የሶፍትዌሩ አካል/ ለምሳሌ የ2000 ብር ተከፋይ ሆነ እንበል። ይህ በሚሆንበት ጊዜ በቁጥር 6 አካውንት ላይ የ2000 ብር ጭማሪ የሚኖረው ሲሆን ሌላ ከየትኛውም የመረቡ አባልም የሚቀነስ አንዳችም ብር አይኖርም ማለት ነው። በተለይም ብዙሀኑ የሚያውቀው የቢትኮይን ስርአተ መረብም በዚህ መልክ ነበር ብሎክቼይንን በመጠቀም ለመጀመሪያ ጊዜ ወደስራ የተተገበረው። በዋናነትም ይህ ሁነት ያስፈልገው ደህንነቱ በተሟላ ሁኔታ እንዲጠበቅ የሚያደረግውን የሚስጥራዊ ስሌት ፍለጋ መረቡ

የሚዘወርበት ስርአት በሚያመነጨው ክፍያ ምክንያትነት የመረቡን ደህንነት ማስጠበቁን እንዲቀጥሉ ያደርጋቸዋል ማለት ነው። ከዚህ ሁነት በኋላ ሁሉም የተስማማበትን አንድ አይነት ገፅ በየራሱ ማህደር ካስቀመጠ በኋላ ቀጣይ ግብይቶችን በአዲስ ገፅ መመዝገብ ይጀምራል ማለት ነው።

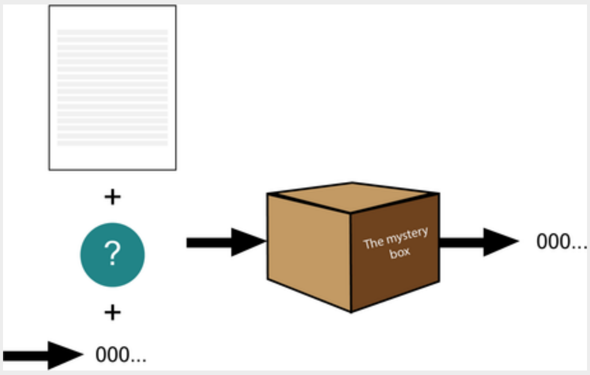
ማስታወሻ : በዚህ ምሳሌ ላይ እንደ ገፅ የወሰድነው ሁነት በብሎክቼይን ስርአቱ ብሎክ/block ብለን የምንጠራውን የግብይት አካል የሚወክልልን ሲሆን የመዘገብነውን ገፆች የምናስቀምጥበትን ማህደር ደግሞ እንደ ቀጣይነት እንዳላቸው ግብይቶችን እንዳስቀመጥንባቸው የገፆች ድምር በመውሰድ በብሎክቼይኑ ስርአታዊ ትርጉም ውስጥ a chain of pages የሚለውን ፅንሰሀሳብ የሚወክለን ይሆናል ማለት ነው። በዚህም የሁለቱ ድምር **ብሎክ-ቼይን/Block-chain** የሚለውን መጠሪያ የሚሰጠን ይሆናል።

በቀላሉ ብሎክቼይን የሚሰራበት መንገድ ይኸው ነው። ይሁንና ከዚህ ባለፈ ማወቅ ያሉብን የተወሰኑ ነጥቦችም አሉ። ለምሳሌ ያህል በምሳሌያችን ላይ የመሰረትነው የብሎክቼይን መረብ ግብይቶችን እያደረገ በመቀጠል 6 የግብይት ገፆችን አጠቃሎ እና ለእያንዳንዱም የመቆለፊያ ኮድ እየሰጠ ወደማህደሩም ዳታውን እያስቀመጠ ግብይቱ ቀጥሏል እንበል። በዚህ ሁነት ላይ ታዲያ አንድ ግለሰብ ወደመጀመሪያው ገፅ ሄዶ የተመዘገቡትን ዳታዎች ለራሱ በሚጠቅም መልኩ ለመለወጥ ቢሞክርስ? ከላይ እንደተገለፀው ለዚህ አይነቱ አጋጣሚ ሁሉም የሚስማማበት መቆለፊያ ኮድ በመኖሩ ምክንያትነት ይህ ሰው ሀሳቡ እንደማይሳካለት ተገልጿል። ይሁንና ግን ይኸው ግለሰብ ለቀየረው ዳታ በእያንዳንዱ ገፅ ላይ የሚገኙትን የመቆለፊያ ስሌቶችም አብሮ መቀየር ቢችልስ? አብዛኛው የብሎክቼይን ቴክኖሎጂን እመርታ የሚጠራጠሩ ሰዎች ጥያቄም ይኸው ነው።

በእርግጥም ብሎክቼይን ደህንነቱ የተጠበቀ የግብይት ምዝገባ ስርአት ነውን?
በእርግጥ ከላይ የተገለፀውን እነዚህን የመቆለፊያ ስሌቶች የመቀየር ሁነት ይበልጡኑ ከአደጋ ሊጠብቃቸው የሚችል የተወሳሰበ ሁነት አለ።
በምሳሌያችን መሀል ከሚስጥራዊው ስሌት መስሪያ ሳጥናችን ሌላ ሁለት ባዶ ሳጥኖች ቢኖሩን ብለን ያነሳናቸውን ሳጥኖች እናስታውስ። አንደኛው በውስጡ 67558 የሚል ቁጥርን በውስጡ የያዘ እንደሆነ እና ሁለተኛው ሳጥን ደግሞ የመቆለፊያ ስሌቱን ለማግኘት የሚረዳድንን ቁጥር ለማወቅ የሚረዳን ባዶ ሳጥን እንደሆነ በምናባችን አስበን ነበር። በእውነታውም ታዲያ በዚህ ስርአት የሚያስፈልጉን ሶስት ሳጥኖች ሲሆኑ እነሱም ሁለቱ ዳታ በውስጣቸው የያዙ ሶስተኛ ደግሞ ባዶ እና ሊታወቅ የሚገባው የመቆለፊያው ስሌት ማስመጫ ናቸው። በዚህም ዋናው የስርአቱ ግብ የነዚህ ሶስት ሳጥኖች ድምር ወደሚስጥራዊው ሳጥን በሚገባበት ወቅት የሚፈለገውን ትክክለኛ እና አብላጫው የመረቡ አባላት የሚስማሙበትን ስሌት ማግኘት ይሆናል።

እስካሁን ባየነው መንገድም ካሉን ሶስት ገፆች መካከል አንዱ ሳጥን አባላቱ የመዘገቡትን የግብይት ዝርዝር የያዘ ሲሆን፤ ሌላኛው ደግሞ የመቆለፊውን ስሌት የያዘ ሳጥን ነው።

ሶስተኛው እና የመጨረሻው ደግሞ ከአንድ መመዝገቢያ ገፅ በፊት የነበረው ገፅ የተቆለፈበት በሚስጥራዊው ሳጥን ያገኘነው የመጨረሻ ውጤት/output/ የምናስቀምጥበት ይሆናል ማለት ነው።



ይህ ብልሀትን ያማከለ አካሄድ በዋናነት እያንዳንዱ የተመዘገቡ እና ተቆልፈው የሚቀመጡ ገፆች የሚተሳሰሩበትን ሊንክ እርስ በእርስ አስተሳሰሮ የሚያስቀምጥ ነው። ይህ የገፆች ማስተሳሰሪያ ሁነት በእርግጥም በግብይት ውስጥ የተመዘገቡ መረጃዎች እና የመቆለፊያ ቁጥሩን ይዘት ለመለወጥ እጅግ አስቸጋሪ የሚያደርገው ይሆናል። በዚህም አንድ ግለሰብ በመረቡ ውስጥ አንድን የተረጋገጠ ገፅ መረጃ ለመቀየር ቢፈልግ ሊቀይረው ካሰበው የመመዝገቢያ ገፅ ጀምሮ አሁን መረቡ እስከደረሰበት የመዝገብ ገፅ ድረስ የተመዘገቡ መረጃዎችን እና መቆለፊያ ቁጥሮችንም መቀየር ይኖርበታል ማለት ነው።

በምሳሌያችን ላይ እንደተመለከትነው በመረቡ ውስጥ ካሉን 20 አባላት መካከል ለምሳሌ አንዱ የብሎክቼይኑን መረጃ የያዘ አንድ ገፅ ላይ የመረጃ ለውጥ ለማድረግ ሙከራ ቢያደርግ ሊለውጠው የፈለገው መረጃ ካለበት ገፅ ጀምሮ እጅግ የበዙ ገፆችን እና አድካሚውን የመቆለፊያ ኮድ ቁጥር በድጋሚ ከስሌት ውስጥ እያስገባ መለወጥም ጭምር ይጠበቅበታል። በዚህም ይህንን መቆለፊያ ቁጥር ለመለወጥ ስሌቱን መስራት እጅጉን ከባድ እና ምናልባትም በግለሰብ ደረጃ ከቶውንም የማይቻል በመሆኑም ይህ ለመረቡ ታማኝ ያልሆነ አንድ ግለሰብ 19ኙ ለመረቡ ታማኝ የሆኑ አባላት የተስማሙበትን ስሌት ለመቀየር የማይቻለው ይሆናል።

ለመረቡ ታማኝ ያልሆነው ይኸው ግለሰብ ለማስተካከል በሚሞክረው ገፅ አማካኝነት የራሱን የሆነ አዲስ ሰንሰለት መፍጠሩ የማቀር ቢሆንም በመረቡ ውስጥ ካሉ የሌሎች የመረጃ ሰንሰለቶች ጋር የሚገጣጠም ዳታ በገፁ ላይ ስለማይኖር በአብላጫው የመረቡ አባላት ስምምነት ላይ

የተደረሰበት ረጅሙ የዳታ ሰንሰለት ምዝገባ ተቀባይነት ያለው እና ታማኝ የሆነው የውሂብ/ዳታ ሰንሰለት ሆኖ የሚቆጠር ይሆናል።

ይሁንና ግን በአንዱ ታማኝ ያልሆነ የመረቡ አባል ፋንታ አብላጫ ድምፅን የሚይዙት አስራ አንዱ አባላት ታማኝነታቸውን ቢያነሱስ ምን ይከሰታል?

በተለያዩ ጊዜያት በብሎክቼይን ቴክኖሎጂ ዙሪያ በሚነገሩ ዜናዎች ላይ የሚደመጠው '51% attack' የተሰኘው ሁነት የሚከሰተው እንዲህ ባሉት አጋጣሚዎች ነው። ይሁንና የብሎክቼይን ቴክኖሎጂ ከጥንስሱ ሲነሳ ከተነሳባቸው እሳቤዎች መካከል በአንድ የብሎክቼይን መረብ ውስጥ የሚገኙ አብላጫው አባላት በመረቡ ላይ ያላቸው የባለቤትነት ድርሻ ከእያንዳንዱ ሌላ አባል ጋር እኩል እንደመሆኑ መጠን ታማኝ ናቸው የሚለው ዋናው እና መሰረታዊ ነው።

ከዚህ በመነሳትም አንድ የብሎክቼይን መረብ ደህንነቱ እና በስራ ላይ የመቆየት ህልውናው ጥያቄ ውስጥ የሚገባው በመረቡ ውስጥ ያሉ አብላጫውን ቁጥር የሚይዙት ግለሰቦች ለመረቡ ያላቸውን ታማኝነት በማንሳት ወደ ኢ-ታማኝነት ሲቀየሩ ብቻ ይሆናል ማለት ነው። ይሄ እና ይሄ የመሳካት ሁነቱ እጅግ አነስተኛ የሆነ ክስተት ካልተከሰተ በቀር የትኛውንም የብሎክቼይን መረብ ለማጥቃትም ሆነ ሰብሮ ለመቆጣጠር፤ አይደለም ሰዎች አለም ላይ ያሉ ሱፐር ኮምፒዩተሮችም የማይቻላቸው ሆኖ እናገኘዋለን።

ፅንሰሀሳቡን ለማስረዳት እጅግ አዳጋች ከሆኑ የሰው ልጅ ስራዎች ሁሉ ከባዱ የሚባለው የብሎክቼይን ቴክኖሎጂ ይህን ይመስላል። ምንም እንኳን እያንዳንዷን የቴክኖሎጂውን ምንነት በነጠረ እና በጣም በቀለለ መለኩ ማስቀመጥ ባይቻል እንኳን እንደመንደርደሪያ ይህች አጭር ፅሁፍ እንደምትረዳ በማሰብም ፅሁፉ በዚህ መልኩ የሚጠናቀቅ ይሆናል።

ስለ ፀሀፊው በትንሹ

ናትናኤል ብሩክ

የክሪፕቶ-ቶክ ኢትዮጵያ ነፃ የክሪፕቶ መማሪያ ኮሚኒቲ መስራች እና ፕሬዘዳንት

የዚች የኪስ መድብል ፀሀፊ ልክ እኤአ በ2017 መባቻ ስለምናባዊ መገበያያ ከረንሲዎች እና ስለተመሰረቱበት የብሎክቼይን ቴክኖሎጂ በአብሮ አደግ ጓደኞቹ አማካኝነት ሰማ። ከቴክኖሎጂ እና ፋይናንስ ነክ ጉዳዮች ጋር ቀረቤታ ስለነበረውም ስለዚህ አዲስ ዓለምን ቀያሪ ቴክኖሎጂ ጭምጭምታ ከታዘበ በኋላ ይበልጥ ለማወቅ ጊዜ፤ ጉልበትና ገንዘቡን በመስኩ ላይ ያተኮሩ ጥናቶችን በማካሄድ ያለውን እውቀት እያዳበረ ለመሄድ ቻለ። ፋይናንሳዊ ነፃነቱንም ለ4 አመታት ክሪፕቶከረንሲዎችን እና መሰል ምናባዊ መገበያዎችን ዕለት ከዕለት በመሸጥ እና በመለወጥ[Day Trading] የሴክተሩ ዘርፍ ላይ በመሰማራት ሊያረጋግጥ ቻለ። ይበልጥ በቴክኖሎጂው ዙሪያ ያለውን እውቀት እና ልምድም ሊያሰፋ ቻለ። በዚህ ሂደት ግን እጅግ አመርቂ የሆነ ስኬትንም የተገኘውን በማጣት ከዘርፉ ጭራሹኑ ለተወሰኑ ጊዜያት እስከመውጣት ብዙ ውጣ ውረዶች የነበሩበትና ፀሀፊውንም በሞራል ስስ ጉዳት አድርሰው ግና በፅናት፤ በትዕግስት፤ በእውቀት፤ በመሳሰሉት እጅግ የበዙ አዎንታዊ ዘላቂ የማንነት ግንባታዎች እንዲገነባ ሊያደርጉት ችለዋል። በሂደትም ይህንኑ እውቀቱን ለአገሩ ልጆች በነፃ ለማካፈል በመወሰንም የክሪፕቶ ቶክ ኢትዮጵያ ነፃ የክሪፕቶከረንሲ እና ብሎክቼይን ቴክኖሎጂን መማሪያ ኮሚዩኒቲ በመመስረት በፋይናንሳዊውም ሆነ በቴክኖሎጂያዊ ትግበራዎች ላይ ያተኮሩ ትምህርቶችን ለኢትዮጵያውን ወጣቶች መስጠት ጀመረ። ናትናኤል በዋናነት ከአዲስ አበባ ዩኒቨርሲቲ የንግድ ስራ ት/ቤት የፋይናንስ እና ዴቨሎፕመንት ኢኮኖሚክስ ምሩቅ ነው። ከምናባዊ መገበያያዎች ግብይት እና ከብሎክቼይን ቴክኖሎጂ ትምህርት ጋር በተያያዘም በሂደት እያየ የመጣውን ቁጥሩ የበዛ ወጣት እውቀት ፈላጊ በመመልከት እና በዘርፉ ለመማር የሚጠየቀው ክፍያ እጅጉን የገዘፈ መሆኑን በማመዛዘን እንደ አንድ አገር ተረካቢ ወጣት አገሩን ለማገልገል፤ በትውልድ ግንባታውም አዎንታዊ አሻራውን ለማሳረፍ በማሰብ ከሙያ አጋሩ ሚስራ ሀሰን ጋር በመሆን የክሪፕቶ ቶክ ኢትዮጵያ ነፃ የክሪፕቶከረንሲ አካዳሚ እና ኮሚዩኒቲ ለመመስረት ቻለ። በዚህም አንዱ የአካዳሚው አላማ መፅሀፎችን በማሳተም እውቀቱ በመላው ሀገሪቱ ተደራሽ እንዲሆን ማድረግ እንደመሆኑ መጠን ይህችን መድብል በነፃ ለሚያስፈልጋቸው አገር ተረካቢ ወጣቶች እንዲደርስ ለህትመት አብቅቶ በተለያዩ የአገሪቷ ክፍሎች ለሚገኙ የመንግስት ትምህርት ቤቶች በነፃ እንዲታደልም አበርክቷል። ከዚሁ ጋር ተያይዞም ጠለቅ ያለ ቴክኒካዊ ሁነቶችን የሚዳስስ የብሎክቼይን መፅሀፍን፤ በዘርፉ በተለይም ከአስገራሚው የቢትኮይን ግብይት ጋር በተያያዘ ያሳለፋቸውን አስገራሚ፤ አስቂኝ፤ አሳዛኝ ሁነቶችን አዋዝቶ የያዘ ግለ ታሪክን ጨምሮ የተለያዩ ለፎሬክስ፤ ስቶክም ሆነ ክሪፕቶ ትሬዲንግ የሚሆኑ የመማሪያ ግብአቶችን ለህትመት በማብቃት አገሩ ለዋለችለት ውለታ መልሱን እየከፈለ የሚገኝ ወጣት ነው።

CRYPTOTALK ETHIOPIA

GET IN TOUCH

+251 910 75 75 72
www.cryptotalket.com
cryptotalket@gmail.com
Telegram : t.me/cte_support