bitcoin

လို - တို - ရှင်း

အိမောင်

Fairway

© Copyright 2021, **Ei Maung**

Fairway Technology. All right reserved.

မာတိကာ

8 **အခန်း (၁) – Bitcoin ဖြစ်ပေါ်လာပုံ**

→ 2008 Financial Crisis

→ Fiat Money

→ Bitcoin စတင်ခြင်း

→ Satoshi Nakamoto ဘယ်သူလဲ

→ လက်ရှိ Bitcoin ကို ဘယ်သူထိန်းချုပ်ထားသလဲ

21 **အခန်း (၂) – Cryptography အကျဉ်း**

→ Encryption

→ Public Key Encryption

→ Hashing

→ Digital Signature

→ Consensus Algorithms

32 **အခန်း (၃) – Bitcoin အလုပ်လုပ်ပုံ**

→ Blockchain

→ Proof of Work

→ Distributed Ledger

→ 51% Attack

→ Coinbase

→ Account (Address)

→ Wallet

→ Bitcoin အချက်အလက်များ

59 **အခန်း (၄) – Mining, Exchanges နှင့် အထွေထွေ**

→ Bitcoin Mining

→ Cryptocurrency Exchanges

→ Bitcoin ဘယ်မှာသုံးလို့ရလဲ

→ ဝေဖန်ချက်နှင့် ကန့်သတ်ချက်များ

79 **အခန်း (၅) – စိတ်ဝင်စားဖွယ်ဖြစ်ရပ်များနှင့် လိမ်လည်မှုများ**

→ Bitcoin Pizza Day

→ ကွိုင်ပျောက်ကြသူများ

→ OneCoin

→ Bitconnect

→ QuadrigaCX

→ ICO Frauds

92 **အခန်း (၆) – Altcoins များ**

→ Litecoin (LTC)

→ Dogecoin (DOGE)

→ Ethereum (ETH)

Smart Contract

ERC–20

ERC–721 (NFT)

ETH vs. ETC

Proof of Stake

→ Cardano (ADA)

→ Polkadot (DOT)

→ Binance Coin (BNB)

→ Ripple (XRP)

→ Uniswap (UNI)

→ Solana (SOL)

→ Chainlink (LINK)

→ Polygon (MATIC)

→ Monero (XMR)

→ Stable Coins (USDT, USDC, BUSD)

→ Dai (DAI)

မိတ်ဆက်

၂၀၀၈ ခုနှစ်၊ နိုဝင်ဘာလ (၁) ရက်နေ့မှာ **Satoshi Nakamoto** ဆိုတဲ့ Pseudonym (ကလောင်အမည်) ကို အသုံးပြုထားသူတစ်ဦးက အစပြုတီထွင်လိုက်တဲ့ Bitcoin ထွက်ပေါ်လာတာဟာ အခုဆိုရင် (၁၀) နှစ်ကျော် သက်တမ်း ရှိသွားပါပြီ။

ကြားခံအဖွဲ့အစည်း မလိုဘဲ တိုက်ရိုက် ဖလှယ်နိုင်သော ဒစ်ဂျစ်တယ် ငွေကြေးစနစ်သစ် ဆိုတဲ့ နိဒါန်းနဲ့ အတူ သက်ဆိုင်ရာ သီအိုရီ Concept များ၊ ဖော်မြူလာများနဲ့တစ်ကွ အသေးစိတ်ရေးသားထားတဲ့ White Paper စာတမ်းတစ်စောင်ကို Cryptography Mailing List တစ်ခုထဲမှာ ဖြန့်ဝေခြင်းအားဖြင့် အစပြုခဲ့တာပါ။ မူရင်း White Paper အပြည့်အစုံကို ဒီလင့်မှာ ဖတ်ရှုနိုင်ပါတယ်။

http://www.bitcoin.org/bitcoin.pdf

အစောပိုင်းမှာ Bitcoin ရဲ့ ဆန်းကျယ်ပြီး လျှို့ဝှက်နက်နဲမှုတို့ကြောင့် –

၁။ နားလည်ရ ခက်ခဲပြီး
၂။ လူတချို့ကသာ စိတ်ဝင်စားတဲ့
၃။ ဒုစရိုက်လောကမှာသာ အသုံးများတဲ့
၄။ တရားမဝင်ငွေကြေး စနစ်တစ်ရပ်လို ဖြစ်နေခဲ့တာပါ။

အခုထိလည်း အဲ့ဒီလိုပဲနေမှာပါလို့ ယူဆနေသူတွေ ရှိနိုင်ပါတယ်။

နားလည်ရခက်တာကတော့ အမှန်ပါ။ အခုထိလည်း ခက်ခဲနေဆဲပါပဲ။ နည်းပညာတွေ ပိုမိုကျယ်ပြန့်လာခြင်းနဲ့အတူ နောက်ကွယ်က အလုပ်လုပ်ပုံတွေက ပိုပြီးတော့တောင် နားလည်ရ ခက်ခဲလာပါသေးတယ်။ ဒီစာအုပ်မှာ အဲ့ဒီ အလုပ်လုပ်ပုံတွေကို အတတ်နိုင်ဆုံး နားလည်ရလွယ်အောင် ရှင်းပြသွားမှာပါ။

နည်းပညာနဲ့ အလုပ်လုပ်ပုံသာမက အစဉ်အလာ ငွေကြေးစနစ်ကနေ လုံးဝခွဲထွက်သွားလို့ သူ့ရဲ့ ငွေကြေးဆိုတဲ့ သဘောသဘာဝကလည်း နားလည်လက်ခံဖို့ ခက်ခဲနေဆဲပါပဲ။ စာရေးသူဟာ စီးပွားရေးဘာသာရပ်ကို ကျွမ်းကျင်တဲ့ ပညာရှင်တစ်ဦး မဟုတ်လို့ အစဉ်အလာ ငွေကြေးစနစ်အကြောင်းကို ကျွမ်းကျင်သူ ရှုထောင့်ကနေတော့ တင်ပြနိုင်မှာ မဟုတ်ပါဘူး။ ဒါပေမယ့် သိသင့်တဲ့ သဘောသဘာဝတွေကို လေ့လာသူ ရှုထောင့်ကနေ ထည့်သွင်း တင်ပြသွားမှာပါ။

ဒီလို နားလည်ရခက်ခဲပေမယ့် လူတချို့ကသာ စိတ်ဝင်စားတဲ့ အရာတစ်ခုတော့ မဟုတ်ပါဘူး။ Tesla လို လုပ်ငန်းမျိုး အပါအဝင် တရားဝင် လုပ်ငန်းကြီးတွေကအစ Bitcoin ကို တန်ဖိုးတက် အရန်စုငွေ Asset Class တစ်ခုအနေနဲ့ ဒေါ်လာဘီလီယံပေါင်းများစွာ ထည့်သွင်း ရင်းနှီးမြှုပ်နှံနေကြသလို အများသူငါရဲ့ စိတ်ဝင်စားမှုကိုလည်း ရရှိနေတဲ့အရာ ဖြစ်နေပါပြီ။ အထူးသဖြင့် Covid-19 ကပ်ရောဂါကြောင့် အများသူငါ အိမ်တွင်းအောင်း နေကြရစဉ်မှာ အိမ်ထဲကနေ လုပ်လို့ရတဲ့ ရင်းနှီးမြှုပ်နှံမှုတွေကို အရင်ကထက် လူတွေပိုပြီး စိတ်ဝင်စားလာကြခြင်းနဲ့အတူ Bitcoin အပါအဝင် Cryptocurrency ရင်းနှီးမြှုပ်နှံမှုတွေကို ပိုမိုစိတ်ဝင်စားလာကြတာကို တွေ့ရပါတယ်။

ပြီးတော့ ဒုစရိုက်လောကမှာသာ သုံးကြတဲ့ တရားမဝင်စနစ်ဆိုတာလည်း မဟုတ်တော့ပါဘူး။ Bitcoin ရဲ့ ဘဏ်မလိုဘဲ တိုက်ရိုက်ဖလှယ်နိုင်မှုကြောင့် ငွေကြေးခဝါချသူတွေ၊ အခွန်ရှောင်သူတွေ၊ မှောင်ခိုသမားတွေ နှစ်သက် အသုံးပြုကြတဲ့အရာ ဖြစ်လိမ့်မယ်လို့ ယူဆခဲ့ကြတာပါ။ လက်တွေ့မှာ Bitcoin ကို အသုံးပြုပြီး ပြုလုပ်တဲ့ ငွေပေးငွေယူ Transaction တွေဟာ အများသူငါ သိရှိနိုင်တဲ့ Public Transaction တွေ ဖြစ်ကြလို့ မသမာမှုတွေမှာအသုံးပြုမယ်ဆိုရင် ပိုပြီးတော့တောင် နောက်ကြောင်းမလုံ ဖြစ်သွားနိုင်ပါသေးတယ်။ ဒါကြောင့်လည်း လက်တွေ့မှာ အမေရိကန်လို နိုင်ငံမျိုးအပါအဝင် နိုင်ငံအတော်များများက Bitcoin ကို အသုံးပြုပြီး ပြုလုပ်တဲ့ ငွေပေးငွေယူ ကိစ္စတွေကို တားမြစ်ထားခြင်း မရှိပါဘူး။

ဆက်ပြီးပြောဖို့လိုလာတာကတော့ Bitcoin ရဲ့ တရားဝင်မှု အခြေအနေပါ။ ဒီကိစ္စကတော့ တစ်နိုင်ငံကို တစ်မျိုးဖြစ်နေလို့ ပြောရခက်ပါတယ်။ အမေရိကန်၊ ဗြိတိန်၊ ဂျပန်၊ တောင်ကိုရီးယား၊ စင်ကာပူ စတဲ့နိုင်ငံတွေ အပါအဝင် ဖွံ့ဖြိုးတဲ့ နိုင်ငံအများစုမှာ Bitcoin နဲ့ Cryptocurrency တွေကို တရားဝင် ငွေကြေးတစ်ရပ် အနေနဲ့ အစိုးရက ကြေညာထားတာမျိုး မဟုတ်ပေမယ့် လွပ်လပ်စွာ အသုံးပြုခွင့် ပေးထားကြပါတယ်။

အခုဒီစာရေးနေစဉ် ရက်ပိုင်းအတွင်းမှာပဲ အယ်ဆာဗေဒိုနိုင်ငံက Bitcoin ဟာ နိုင်ငံရဲ့ တရားဝင်ငွေကြေး ဖြစ်ကြောင်း ကြေညာထားပါတယ်။ ဒီကြေညာချက်ရဲ့ နောက်ကွယ်မှာလည်း စိတ်ဝင်စားစရာတွေ ရှိနေပါတယ်။ အယ်ဆာဗေဒိုနိုင်ငံဟာ အမေရိကန်ဒေါ်လာကို အဓိကငွေကြေးအနေနဲ့ အသုံးပြုနေရတဲ့အတွက် သူ့အစိုးရမှာ ငွေကြေးအပေါ် တိုက်ရိုက်ထိန်းချုပ်နိုင်စွမ်း မရှိပါဘူး။ ပြီးတော့ နိုင်ငံရဲ့ ဝင်ငွေအများစုဟာ ပြည်ပထွက် အလုပ်လုပ်ကြသူတွေ ပြန်လွှဲပို့တဲ့ငွေတွေ ဖြစ်နေပါတယ်။ နိုင်ငံသားအများစုဟာ ဘဏ်အကောင့်မရှိကြသူတွေ ဖြစ်တဲ့အတွက် လွှဲပို့ငွေထုတ်ယူဖို့ နာရီပေါင်းများစွာ သွားရတာတွေ၊ များပြားတဲ့ နိုင်ငံခြား ငွေလွှဲခကို ပေးရတာတွေ၊ စတဲ့ပြဿနာတွေကို ရင်ဆိုင်နေရတာပါ။ ဒီပြဿနာတွေကို ဘဏ်အကောင့်မလိုဘဲ တိုက်ရိုက်ပေးပို့လက်ခံနိုင်တဲ့ Bitcoin ကို အသုံးပြုလိုက်ခြင်းအားဖြင့် အမှန်တစ်ကယ် ဖြေရှင်းနိုင်မလား ဆိုတာတော့ စောင့်ကြည့်ကြရမှာပါ။ အယ်ဆာဗေဒိုလိုပဲ အမေရိကန်ဒေါ်လာကို မှီခိုနေရတဲ့ အိမ်နီးချင်း ဗဟိုအမေရိက နဲ့ လက်တင်အမေရိက နိုင်ငံတွေကလည်း ဒီအခြေအနေကို စောင့်ကြည့်နေကြပါတယ်။

အယ်ဂျီးရီးယား၊ အီဂျစ်နဲ့ မော်ရိုကို တို့လိုနိုင်ငံတွေကတော့ Bitcoin နဲ့ Cryptocurrency တွေကို လုံးဝ တရားမဝင်ဘူးလို့ အတိအလင်း သတ်မှတ်ထားပါတယ်။ ကနေဒါ၊ ဆော်ဒီအာရေးဗီးယား၊ တူရကီ တို့လို နိုင်ငံတွေလို အများပြည်သူကို မတားမြစ်ပေမယ့် ဘဏ်နဲ့ ငွေကြေးအဖွဲ့အစည်းတွေကို တားမြစ်ထားတဲ့ နိုင်ငံတွေလည်း ရှိပါတယ်။ အိန္ဒိယလို နိုင်ငံမျိုးမှာတော့ အစိုးရ ကြေညာချက်ကိုယ်တိုင်က မရှင်းလို့ တရားဝင်ခြင်း၊ မဝင်ခြင်းဟာ အခုထိ အငြင်းပွားနေဆဲပါပဲ။ တရုတ်နဲ့ ရုရှားလို နိုင်ငံတွေမှာလည်း ကန့်သတ်ချက်တွေရှိနေလို့ တရားဝင်တယ်၊ မဝင်ဘူး ပြောရခက်တဲ့ အနေအထားမှာ ရှိနေကြပါတယ်။ ဒါကြောင့် တချို့နိုင်ငံတွေမှာ တရားဝင်ပြီး တချို့နိုင်ငံတွေမှာ တရားမဝင်ဘူးလို့သာ ပြောနိုင်ပါတယ်။ Bitcoin ရဲ့ တရားဝင်မှု အခြေအနေစာရင်းကို ဒီလိပ်စာမှာ ကြည့်လို့ရပါတယ်။

https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country_or_territory

အဲ့ဒီစာရင်းမှာ ကြည့်လိုက်ရင် မြန်မာနိုင်ငံကတော့ No Data ဖြစ်နေပါလိမ့်မယ်။ ဒါပေမယ့် မြန်မာနိုင်ငံမှာလည်း ၂၀၁၉ ခုနှစ်၊ မေလ (၃) ရက်နေ့ ရက်စွဲ နဲ့ ထုတ်ပြန်ခဲ့တဲ့ ဗဟိုဘဏ်ရဲ့ အသိပေးကြေညာချက်အရ Bitcoin အပါအဝင် Cryptocurrency တွေကို တရားဝင်ငွေကြေးအဖြစ် အသိအမှတ်ပြုထားခြင်း မရှိသလို ငွေကြေးအဖွဲ့အစည်းများကို ရောင်းဝယ် လဲလှယ်ခွင့်လည်း ပြုမထားဘူးလို့ ဆိုပါတယ်။ တားမြစ်ချက်တွေကို ဖောက်ဖျက်ရင် တရားစွဲဆိုသွားမှာဖြစ်ကြောင်းကိုလည်း အမိန့်ကြော်ငြာစာအမှတ် ၉/၂၀၂၀ နဲ့လည်း ဆက်ထုတ်ပြန် ထားပါသေးတယ်။

ဒါကြောင့် ဒီစာရေးနေချိန်အထိ Bitcoin အပါအဝင် Cryptocurrency တွေဟာ မြန်မာနိုင်ငံမှာ တရားဝင်ငွေကြေးအဖြစ် အသိအမှတ်ပြုထားခြင်း မရှိသလို၊ ငွေကြေးအဖွဲ့အစည်းတွေကို ရောင်းဝယ် လဲလှယ်ခွင့်လည်း ပြုမထားဘူး ဆိုတာ အထူး သတိပြုရမှာ ဖြစ်ပါတယ်။

ဒီစာအုပ်မှာ Bitcoin နဲ့ Cryptocurrency တွေ အရောင်းအဝယ်၊ အလဲအလှယ် ပြုလုပ်နည်းတွေကို ဖော်ပြသွားမှာ မဟုတ်သလို၊ အရောင်းအဝယ်၊ အလဲအလှယ်လုပ်ဖို့ အားပေးခြင်းလည်း (လုံးဝ) မဟုတ်ပါဘူး။ နားလည်ရ ခက်ခဲတဲ့ Bitcoin နဲ့ Cryptocurrency တွေရဲ့ နည်းပညာပိုင်း အလုပ်လုပ်ပုံကိုသာ အသိပညာပေးစာအုပ် အနေနဲ့ ဖော်ပြသွားမှာပဲ ဖြစ်ပါတယ်။

အခန်း (၁) – Bitcoin ဖြစ်ပေါ်လာပုံ

ပြီးခဲ့တဲ့အခန်းမှာ ပြောခဲ့သလိုပဲ Bitcoin ကို ၂၀၀၈ ခုနှစ်၊ နိုဝင်ဘာလ (၁) ရက်နေ့မှာ Satoshi Nakamoto ဆိုတဲ့ ကလောင်အမည်ကို အသုံးပြုထားသူတစ်ဦးက Cryptography Mailing List တစ်ခုမှာ အိုင်ဒီယာ အသေးစိတ်ကို White Paper နဲ့တစ်ကွ ဖြန့်ဝေခြင်းအားဖြင့် စတင်ခဲ့တာ ဖြစ်ပါတယ်။

၂၀၀၈ ခုနှစ်ဟာ ကမ္ဘာ့စီးပွားရေးအတွက် ထူးခြားအရေးပါတဲ့ နှစ်တစ်နှစ်ပါ။ အမေရိကန်နိုင်ငံရဲ့ အိမ်ခြံမြေ ဈေးကွက် ပြိုလဲခြင်းရဲ့ နောက်ဆက်တွဲ ရိုက်ခတ်မှုနဲ့အတူ ကမ္ဘာ့ငွေကြေးစီးပွားပျက်ကပ်ကြီးကို ရင်ဆိုင်ခဲ့ကြရတဲ့ နှစ်တစ်နှစ်ပဲ ဖြစ်ပါတယ်။ 2008 Financial Crisis လို့ ခေါ်ကြသလို 2008 Housing Crisis လို့လည်း ခေါ်ကြပါတယ်။ 2008 Subprime Mortgage Crisis လို့လည်း ခေါ်ကြပါသေးတယ်။

2008 Financial Crisis

၂၀၀၈ ခုနှစ် ကမ္ဘာ့ငွေကြေးစီးပွားပျက်ကပ်ရဲ့ ရိုက်ခတ်မှုကြောင့် အမေရိကန်နဲ့ ကမ္ဘာအနှံ့အပြားမှာ အိမ်ခြံမြေဈေးတွေ ထိုးကျပြီး ဘဏ်နဲ့ ငွေကြေးအဖွဲ့အစည်းတွေ ဒေဝါလီခံခဲ့ကြရပါတယ်။ ဘဏ်တွေအပေါ် လူတွေရဲ့ ယုံကြည်မှုပျက်ပြားသွားခြင်းအပါအဝင် နောက်ဆက်တွဲ ရိုက်ခတ်မှုတွေကြောင့် စီးပွားရေးလုပ်ငန်းတွေ ပျက်ကြရပြီး လူသန်းပေါင်းများစွာ အလုပ်လုပ်မဲ့ဖြစ်ကြရ၊ အိုးမဲ့အိမ်မဲ့တွေ ဖြစ်ခဲ့ကြရပါတယ်။ IMF ရဲ့ ခန့်မှန်းချက်အရ အမေရိကန်နဲ့ ဥရောပဘဏ်တွေရဲ့ ဆုံးရှုံးမှုဟာ ဒေါ်လာ (၁) ထရီလီယံ အထိ ရှိခဲ့တယ်လို့ ဆိုပါတယ်။ ဒါဟာ ၂၀၀၈ ခုနှစ်ရဲ့ ဆုံးရှုံးမှုပမာဏဖြစ်ပြီး စီးပွားပျက်ကပ်အကြိုနဲ့ နောက်ဆက်တွဲ ကာလကိုပါ ထည့်တွက်ရင် ဒီထက် ပိုပါလိမ့်ဦးမယ်။ ဒီဆုံးရှုံးနစ်နာမှုတွေဟာ ငွေကြေးစီမံခန့်ခွဲသူတွေရဲ့ လိုတာထက်ပိုတဲ့ အလွန်အကျွံ စွန့်စားမှုတွေကြောင့် ဖြစ်ခဲ့ရတာ ဖြစ်သလို၊ ဒီအဖွဲ့အစည်းတွေကို စောင့်ကြည့်ကြီးကြပ်ရမယ့် သက်ဆိုင်ရာအာဏာပိုင်တွေရဲ့ တာဝန်ပျက်ကွက်မှုကြောင့် လို့လည်း ဆိုကြပါတယ်။

သာမန်အားဖြင့် ဘဏ်တွေက ပုံမှန်ဝင်ငွေရှိပြီး မှတ်တမ်းကောင်း ရှိတဲ့သူတွေကို ချေးငွေစာချုပ်နဲ့ အိမ်အရစ်ကျ ဝယ်ခွင့်ပေးကြပါတယ်။ ဒါက မထူးဆန်းပါဘူး။ ထူးဆန်းတာကတော့ စုငွေစီမံခန့်ခွဲမှု နဲ့ ရင်းနှီးမြှုပ်နှံမှု အဖွဲ့အစည်း Hedge Fund တွေက အဲ့ဒီအိမ်ချေးငွေ စာချုပ်တွေကို ဘဏ်တွေဆီကနေ တစ်ဆင့်ပြန် ဝယ်ယူခြင်းပဲ ဖြစ်ပါတယ်။ ဒီသဘောသဘာဝဟာ Mortgage Backed Security တို့ Collateralize Debt Obligations တို့လို ပညာရပ်ပိုင်း အသုံးအနှုန်းတွေနဲ့အတူ အတော်လေး ကျယ်ပြန့်ပေမယ့် လိုရင်းကတော့ ပင်စင်စုငွေလို ငွေလုံးငွေရင်းကို ကိုင်တွယ်စီမံရတဲ့ အဖွဲ့အစည်းတွေက အဲ့ဒီငွေတွေ တိုးပွားအောင် နည်းလမ်းအမျိုးမျိုးနဲ့ ကြံဆကြရာမှာ၊ အတိုးလည်း ကောင်းကောင်းရပြီး အိမ်အပေါင် ရှိနေလို့ အတန်အသင့်လည်း စိတ်ချရတဲ့ အရစ်ကျ အိမ်ချေးငွေစာချုပ်တွေကို ဘဏ်တွေဆီကနေ တစ်ဆင့်ပြန် လိုက်ဝယ်တာပါ။ ဒီလုပ်ငန်းတွေဟာ ပုံမှန်အားဖြင့် အတိုးနှုန်းနည်းပေမယ့် ပိုစိတ်ချရတဲ့ အစိုးရ ငွေတိုက်စာချုပ်လိုမျိုးတွေမှာသာ ရင်းနှီးမြှုပ်ကြလေ့ရှိတာပါ။

အစောပိုင်းမှာ ဒီနည်းဟာ အလုပ်ဖြစ်ပြီး အတိုးများများရတဲ့အတွက် ချေးငွေစာချုပ်တွေ ပိုပြီးတော့ အဝယ်လိုက်လာကြသလို၊ ဘဏ်တွေဘက်ကလည်း အရင်ထက်ပိုပြီး အိမ်အရစ်ကျ ချေးငွေတွေကို ပိုပြီးတော့ ထုတ်ပေးလာပါတယ်။ လူတွေ ချေးငွေပိုယူလာအောင် အတိုးနှုန်းတွေလျှော့ပြီး ချေးပေးပါတယ်။ ပုံမှန်ဝင်ငွေ မကောင်းတဲ့သူတွေ၊ အရင်က အကြွေးမှတ်တမ်းကောင်း မရှိတဲ့သူတွေကိုပါ ထုတ်ချေးလာတဲ့ အထိ ဖြစ်လာတာပါ။ အဲ့ဒီလို ချေးငွေမျိုးကို Subprime Mortgage လို့ ခေါ်ကြတာပါ။ ဒီလို ဖောဖောသီသီ ထုတ်ချေးရာကနေ အလွန်အကျွံအဆင့် ဖြစ်လာပြီး ပုံမှန်ဝင်ငွေ မပြနိုင်တဲ့သူတွေကို ထုတ်ချေးတဲ့အဆင့်ထိ ရောက်လာပါတော့တယ်။ ဒီအချိန်ထိ အိမ်အရစ်ကျချေးငွေအတွက် အိမ်တစ်လုံးလုံး အပေါင်ရှိနေလို့ စိတ်ချရတယ်လို့ ယူဆနေကြဆဲပါပဲ။

ဖောဖောသီသီ ချေးငွေထုတ်ပေးနေလို့ အိမ်တွေရောင်းကောင်းပြီး အိမ်ဈေးတွေကလည်း ထိုးတက်လာပါတယ်။ အဲ့ဒီလို ထိုးတက်နေလေ အိမ်အပေါင်နဲ့ ငွေချေးပေးရတာ စိတ်ချရတယ်လို့ ယူဆရလေပါပဲ။ ချေးငွေယူထားသူက ပြန်မဆပ်ခဲ့ရင် ဈေးတက်နေတဲ့ အိမ်ကိုသိမ်းပြီး ငွေပြန်ဖော်လို့ ရနိုင်တယ်ဆိုတဲ့ သဘောပါ။ ဒီတော့ ထပ်တိုးပြီးတော့ ထုတ်ချေးပေးလာကြပါတယ်။

ဒါပေမယ့် မကြာပါဘူး။ နောက်ဆုံးမှာ ပြန်မဆပ်နိုင်ဘဲ ယူထားတဲ့ ချေးငွေတွေများလာတာနဲ့အမျှ ပြန်မဆပ်နိုင်တဲ့သူတွေလည်း များလာပါတော့တယ်။ အပေါင်ဆုံးအိမ်တွေ တစ်လုံးပြီးတစ်လုံးကို ငွေဖော်ဖို့ ပြန်ထုတ် ရောင်းလာကြရတဲ့အခါ ရောင်းလိုအားနဲ့ ဝယ်လိုအား မမျှတော့ဘဲ အိမ်ဈေးတွေဟာ ဖောက်ထိုးပြန်

ကျဆင်းတော့တာပါပဲ။ ဒီလိုအိမ်ဈေးတွေ ပြန်ထိုးကျတဲ့အခါ၊ မူလဈေးကြီးနဲ့ ချေးငွေယူထားမိသူတွေဟာ သူတို့အိမ် တန်ဖိုးကျသွားပြီဖြစ်လို့ ချေးငွေကို ပြန်ဆပ်မယ့်အစား အဆုံးခံလိုက်တာကမှ ပိုတန်သလို ဖြစ်နေတဲ့အတွက် ပြန်မဆပ်ကြတော့တာတွေထိ ရှိလာပါတယ်။ အဲ့ဒီမှာ အပေါင်ဆုံးအိမ်တွေ ထပ်တိုးလာပြီး ငွေးဖော်ဖို့ ထပ်တိုးပြီး ထုတ်ရောင်းလာကြရတဲ့အတွက် ဈေးတွေကျပြီးရင် ထပ်ကျပြန်ပါတယ်။

နောက်ဆုံးမှာ ထုတ်ပေးထားတဲ့ချေးငွေနဲ့ ပြန်ရတဲ့ငွေ ဘယ်လိုမှမကာမိတော့ဘဲ၊ ရင်းနှီးမြှုပ်နှံသူတွေလည်း ချေးငွေတွေဆုံး အရှုံးကြီးရှုံးပြီး ဒေဝါလီ ခံကုန်ကြပါတော့တယ်။ ဒီလိုမျိုး ချေးငွေဆုံးလို့ အရှုံးပေါ်တာမျိုးတွေ အတွက် အာမခံပေးတဲ့ အာမခံလုပ်ငန်းတွေလည်း မလျော်နိုင်တော့လို့ အထိနာကြပြန်ပါတယ်။ ဒါတွေဟာ တစ်ခုနဲ့တစ်ခု ဆက်စပ်နေကြတာဖြစ်လို့ သက်ရောက်မှုက ကဏ္ဍစုံကို ပြန့်နှံ့သွားတာပါ။ Lehman Brothers လို သက်တမ်းရင့် ဘဏ်ကြီးလည်း ဒေဝါလီ ခံသွားရပါတယ်။ ဒီအခါမှာ လူတွေက ဘဏ်တွေအပေါ်မှာ ယုံကြည်မှု ပျက်သွားပါတော့တယ်။ ငွေတွေ အမြန်ပြန်ထုတ်ကြလို့ တစ်ခြားဘဏ်တွေကိုပါရိုက်ခတ်လာပါတယ်။ အမေရိကန်နိုင်ငံမှာ အစပြုခဲ့တဲ့ ဒီပြဿနာဟာ ကမ္ဘာ့အနှံ့ကို ပျံ့နှံ့သွားပါတယ်။

ဒီအခါကျတော့မှ ဗဟိုဘဏ်တွေ နဲ့ အာဏာပိုင်တွေက အခြေအနေကို အပြေးအလွှား ဝင်ထိန်းရပါတယ်။ ငွေစက္ကူအသစ်တွေ ရိုက်ထုတ်ပြီး ဘဏ်တွေကို ငွေချေးပေးပါတယ်။ လူတွေရဲ့ ယုံကြည်မှုအတွက် ဘဏ်တွေဘက်က ဝင်ပြီးတော့ အာမခံပေးပါတယ်။ အပေါင်ဆုံးအိမ်တွေကို အစိုးရက ဝင်ဝယ်ပေးပါတယ်။ ချေးငွေစာချုပ်တွေကိုလည်း ဝင်ပြီးတော့ ဝယ်ပေးကြပါတယ်။ ဒီအစီအစဉ်တွေကြောင့် စီးပွားပျက်ကပ်ကိုတန့်သွားအောင် အချိန်မီ ထိန်းလိုက်နိုင်ပေမယ့် ထိခိုက်နစ်နာသူတွေကတော့ နစ်နာသွားကြပါပြီ။

ရင်းနှီးမြှုပ်နှံမှုလုပ်ငန်းတွေရဲ့ အလွန်အကျွံစွန့်စားမှုကြောင့် အတိုးအမြတ် များများရရင် မန်နေဂျာတွေက ဘောနပ်တွေအများကြီး ရကြပါတယ်။ အခုလို ဆုံးရှုံးနစ်နာမှုတွေ ဖြစ်တဲ့အခါမှာတော့ စုငွေပိုင်ရှင် အများပြည်သူကသာ နစ်နာတာပါ။ ဘဏ်တွေအနေနဲ့လည်း အစိုးရက အပြိုမခံနိုင်လို့ သူတို့ကိုပစ်မထားဘူး၊ မဖြစ်မနေ ဝင်ထိန်းပေးရမယ် ဆိုတာသိလို့ လိုတာထက်ပိုပြီး စွန့်စားကြတာပါ။ နောက်ဆုံး ဒီလိုမျိုး မတည်ငြိမ်မှုတွေကြောင့် တစ်ကယ်နစ်နာပြီး ကျန်ခဲ့တာကတော့ အများပြည်သူပဲ ဖြစ်ပါတယ်။

ဒီလို ဗဟိုငွေကြေးထိန်းချုပ်မှုစနစ်ရဲ့ အကျင့်ပျက်မှုနဲ့ အားနည်းချက်တွေကြောင့် အစဉ်အလာငွေကြေးကို အစားထိုးနိုင်ဖို့ ကြားခံအဖွဲ့အစည်းမလိုဘဲ တိုက်ရိုက်ဖလှယ် အပေးအယူလုပ်နိုင်ပါတယ်ဆိုတဲ့ ဒစ်ဂျစ်တယ်ငွေကြေးစနစ် Bitcoin ကို Satoshi Nakamoto က တီထွင်ခဲ့တာပါ။

Fiat Money

ဒီနေရာမှာ အစဉ်အလာ ငွေကြေးစနစ်အကြောင်းကို အနည်းငယ်ထည့်ပြောချင်ပါတယ်။ ငွေကြေးပိုက်ဆံဆိုတာ မပေါ်ခင် ဟိုးရှေးခေတ်က ဘာတာ စနစ်ခေါ် ပစ္စည်းခြင်း တိုက်ရိုက်ဖလှယ်တဲ့ စနစ်ကို သုံးခဲ့ကြတယ်ဆိုတာ ကြားသိဖူးကြမှာပါ။

တိုက်ရိုက်ဖလှယ်တယ်ဆိုတာ အဆင်မပြေပါဘူး။ ဂေါ်ဖီတစ်ထုတ်နဲ့ ဆိတ်တစ်ကောင် လဲလို့ မရနိုင်ပါဘူး။ တန်ဖိုးခြင်း မမျှပါဘူး။ တန်ဖိုးခြင်းမျှသွားအောင် (ဥပမာ) ဂေါ်ဖီထုတ် တစ်ရာနဲ့ ဆိတ်တစ်ကောင် လဲမယ်ဆိုရင်လည်း ဆိတ်ပိုင်ရှင်က ဂေါ်ဖီထုတ်တစ်ရာ သူ့အတွက် အသုံးမလိုလို့ လဲချင်မှာ မဟုတ်ပါဘူး။ ဒါကြောင့် တိုက်ရိုက်ဖလှယ်တဲ့စနစ်ကို စီးပွားဖြစ် သုံးကြတာမျိုး မဟုတ်ဘဲ မဖြစ်မနေလိုအပ်လာတဲ့အခါ လဲလှယ်ကြတဲ့ သဘောမှာပဲ ရှိခဲ့ကြတာပါ။ လူတိုင်းက ကိုယ့်စားဝတ်နေရေးအတွက် လိုအပ်တာကို ကိုယ်တိုင်ပဲ အကုန် ထုတ်လုပ်ကြရတာပါ။ ပေါက်တူး၊ ဂေါ်ပြား လုပ်တာကျွမ်းကျင်လို့ ပန်းပဲဖိုထောင်ပြီး ပေါက်တူး ဂေါ်ပြားတွေချည်းပဲ ထိုင်လုပ်နေလို့ မရနိုင်ပါဘူး။ ရလာတဲ့ ပေါက်တူး၊ ဂေါ်ပြားကို စားစရာနဲ့ ဖလှယ်ရတာအဆင်မပြေလို့ ကိုယ်တိုင်လည်း လယ်စိုက်ရဦးမှာပါ။ ဒီသဘောကြောင့် လူသားတွေရဲ့ အထွေထွေ ဖွံ့ဖြိုးတိုးတက်မှုဆိုတာလည်း နှေးကွေးခဲ့ကြပါတယ်။

နောက်ပိုင်းမှာတော့ တချို့အများသဘောတူတဲ့ အရာတွေကို ကြားခံထားပြီး ဖလှယ်လားကြပါတယ်။ ဒေသတစ်ခုနဲ့တစ်ခု၊ ခေတ်တစ်ခုနဲ့တစ်ခု၊ အသုံးပြုကြတဲ့ ကြားခံပစ္စည်းကတော့ မတူကြပါဘူး။ ဥပမာ – ဂေါ်ဖီတစ်ထုတ်ကို ရှားပါးပင်လယ် ခရုခွံ တစ်ခုနဲ့လဲရပြီး ဆိတ်တစ်ကောင်ကို ခရုခွံ အခုတစ်ရာနဲ့ လဲရမယ်လို့ အများက လက်ခံထားရင်၊ ဆိတ်ပိုင်ရှင်က သူ့ဆိတ်ကထွက်တဲ့ နို့တစ်ပုလင်းကို ခရုခွံတစ်ခုနဲ့ လဲပြီး ရလာတဲ့ခရုခွံနဲ့ လိုချင်တဲ့ဂေါ်ဖီထုတ်ကို ပြန်လဲယူလို့ ရသွားပါပြီ။ ဂေါ်ဖီထုတ်လိုချင်ယုံနဲ့ သူ့ဆိတ်တစ်ကောင်လုံးကို ပေးလိုက်စရာ မလိုတော့ပါဘူး။ ဒီနည်းနဲ့ ကြားခံဖလှယ်နိုင်စွမ်းရှိတဲ့ ငွေကြေးဆိုတာ ထွက်ပေါ်လာပါတော့တယ်။

ဒီလိုကြားခံစနစ် ရှိလာတဲ့အခါ လူတွေက ကိုယ်ကျွမ်းကျင်ရာကို ဇောက်ချ အလုပ်လုပ်နိုင်သွားပါပြီ။ ပေါက်တူး၊ ဂေါ်ပြားလုပ်တာ ကျွမ်းကျင်တဲ့သူက ပန်းပဲဖိုထောင်ပြီး အရည်အသွေးကောင်းတဲ့ ပေါက်တူး၊ ဂေါ်ပြားတွေ အများကြီး ထုတ်လုပ်ပြီး ခရုခွံနဲ့လဲ၊ ရတဲ့ ခရုခွံနဲ့ စားဝတ်နေရေးအတွက် လိုအပ်တာတွေ ပြန်လဲယူလို့ ရသွားတဲ့အတွက် သူကိုယ်တိုင် လယ်စိုက်နေစရာ မလိုတော့ပါဘူး။ တစ်ခြား ပေါက်တူး ဂေါ်ပြား လိုအပ်သူတွေလည်း ပေါက်တူးတစ်လက်အတွက် ကိုယ်တိုင် ပန်းပဲဖိုဆောက် နေစရာမလိုတော့ဘဲ သူ့

လယ်ကထွက်တဲ့ စားစရာရောင်းလို့ရတဲ့ ခရုခွံနဲ့ လိုအပ်တဲ့ ပေါက်တူးကို လဲယူလို့ ရသွားပါပြီ။ ဒီနည်းနဲ့ ကျွမ်းကျင်ရာကို အာရုံစိုက်ကြလို့ ကုန်ထုတ်စွမ်းအား တိုးတက်လာပြီး ဒေသဖွံ့ဖြိုးမှုနဲ့ လူနေမှု အဆင့်အတန်းတွေလည်း အလျှင်အမြန် တိုးတက်လာကြတာပါ။

ဒီလိုကြားခံဖလှယ်ဖို့ ဆက်လက်ပြီး အသုံးများလာကြတာကတော့ ရွှေ နဲ့ ငွေ ပဲဖြစ်ပါတယ်။ ရွှေနဲ့ငွေတို့ဟာ ရှားပါး၊ အကြမ်းခံ၊ လှပပြီး၊ လိုရာ ပုံသွင်းယူလို့ရတဲ့ ဂုဏ်သတ္တိတွေ ရှိကြလို့ အလွန် အဖိုးတန်ပါတယ်။ အဲ့ဒီလို အဖိုးတန်ရွှေ နဲ့ ငွေတို့ကို အစိတ်အပိုင်းလေးတွေလုပ်၊ ဒင်္ဂါးပြားအဖြစ် ပုံသွင်းပြီး ကြားခံဖလှယ်နိုင်တဲ့ ငွေကြေးအနေနဲ့ လက်ခံ အသုံးပြုကြတာပါ။

ကိုယ့်ရွှေကို ပန်းထိန်ဆိုင်တစ်ဆိုင်မှာ ဒင်္ဂါးပြားလုပ်ဖို့ အပ်ထားတဲ့အခါ ပန်းထိန်ဆိုင်က ဘောင်ချာသဘောမျိုး လက်ခံစက္ကူစာရွက် ပြန်ထုတ်ပေးပါတယ်။ အဲ့ဒီစာရွက်ပါရင် ရွှေဒင်္ဂါးကို ပြန်ထုတ်ပေးမယ်လို့ အာမခံတဲ့ သဘောပါ။ ဒီတော့ တစ်ခုခုဝယ်ဖို့ ဒင်္ဂါးပြားအသင့် မရှိသေးရင်လည်း အဲ့ဒီဘောင်ချာစက္ကူကိုပဲ ပေးလိုက်လို့ရပါတယ်။ လက်ခံတဲ့သူကလည်း ဒီစက္ကူနဲ့ ရွှေဒင်္ဂါး ပြန်ထုတ်လို့ရတာ ယုံကြည်တဲ့အတွက် လက်ခံတဲ့အခါ ကြားခံဖလှယ်တာ ဒင်္ဂါးပြား မဟုတ်တော့ဘဲ ပန်းထိန်ဆိုင်ရဲ့ လက်ခံစက္ကူ ဖြစ်သွားပါပြီ။ အဲ့ဒီကနေ ကနေ့အသုံးပြုနေကြတဲ့ ငွေစက္ကူနဲ့ ကြားခံဘဏ်ရယ်လို့ အဲ့ဒီမှာ အစပြု ဖြစ်ပေါ်လာကြတော့တာပါ။ ပန်းထိန်ဆိုင်က ထုတ်ပေးတဲ့ ဘောင်ချာစက္ကူဟာ ငွေစက္ကူဖြစ်သွားပြီး၊ ပန်းထိန်ဆိုင်ကတော့ ကြားခံဘဏ်ဖြစ်သွားပါပြီ။

(၁၇) ရာစုလောက် ရောက်တဲ့အခါ ရွှေ ကို စံထားပေမယ့် ငွေစက္ကူ ကိုသာ ကြားခံဖလှယ်ဖို့အတွက် အသုံးပြုတဲ့ ငွေကြေးစနစ်တွေ အတော်လေးကျယ်ပြန့်လာခဲ့ပါပြီ။ ဘဏ်တွေက ထုတ်ပေးထားတဲ့ ငွေစက္ကူနဲ့ တန်ဖိုးညီမျှတဲ့ အရန်ရွှေကို မီးခံသေတ္တာကြီးတွေထဲမှာ သိမ်းထားပြီး လိုအပ်ရင်အချိန်မရွေး ငွေစက္ကူကို ရွှေနဲ့ ပြန်လဲပေးမယ်ဆိုတဲ့ အာမခံချက်နဲ့အတူ အသုံးပြုခဲ့ကြတာပါ။ ထူးထူးခြားခြား ဗြိတိန်မှာတော့ ရွှေ အစား ငွေကို စံထားပါတယ်။ ဗြိတိန်ရဲ့ ငွေစက္ကူကို စတာလင်ပေါင်လို့ ခေါ်ကြတာဟာ Sterling Silver ခေါ် ငွေသတ္တုကို စံထားပြီး ထုတ်ပေးရာကနေ ဖြစ်ပေါ်လာတာပါ။ စတာလင်ပေါင် (၁) ပေါင်ဟာ Sterling Silver (၁) ပေါင်နဲ့ တန်ဖိုးညီမျှတယ်ဆိုတဲ့ သဘောပါ။

ဘဏ်တွေဟာ အဲ့ဒီလို ရွှေကို အရန်ထားပြီး တန်ဖိုးညီတဲ့ ငွေစက္ကူကိုသာ ဖြန့်ဝေကြလို့ အဲ့ဒီငွေစက္ကူတွေဟာလည်း ရွှေကဲ့သို့ နောက်ခံတန်ဖိုး အစစ်အမှန် ရှိနေတယ်လို့ ဆိုနိုင်ပါတယ်။ ဒါပေမယ့် နောက်ပိုင်းမှာတော့ စီးပွားရေး အလျှင်အမြန် ဖွံ့ဖြိုးတိုးတက်လာခြင်းနဲ့အတူ၊ ရွှေ ရှားပါးလာမှု၊ ငွေစက္ကူ လိုအပ်ချက် မြင့်တက်လာမှုတွေနဲ့အတူ ငွေစက္ကူကို အရန်ရွှေနဲ့ ချိတ်ဆက်ခြင်း မပြုနိုင်ကြတော့ဘဲ ဘဏ်ရဲ့အာမခံချက်၊ အစိုးရရဲ့ အာမခံချက်နဲ့ ရိုက်ထုတ်လာကြရပါတယ်။ အမေရိကန်နိုင်ငံဟာ သမ္မတနစ်ဆင်လက်ထက် (၁၉၇၁) ခုနှစ်မှာ ဒေါ်လာကို ရွှေနဲ့ချိတ်ဆက်ထားခြင်းကနေ ရပ်ဆိုင်းလိုက်ကြောင်း ကြေညာခဲ့ပါတယ်။

အဲ့ဒီလို အစိုးရအမိန့်အာဏာသက်သက်၊ အာမခံချက်သက်သက်နဲ့ ထုတ်တဲ့ ငွေကြေးကို Fiat Money (သို့) Fiat Currency လို့ ခေါ်ကြတာပါ။ ဒီငွေကြေးမှာ နောက်ခံတန်ဖိုး အစစ်ဆိုတာ မရှိပါဘူး။ အများက တန်ဖိုးရှိတယ်လို့ လက်ခံကြလို့သာ တန်ဖိုးရှိနေတာဖြစ်ပြီး၊ အစိုးရက တန်ဖိုးရှိတယ်လို့ အမိန့်ထုတ်ထားလို့သာ တန်ဖိုးရှိနေကြတာ ဖြစ်ပါတယ်။ ဒီငွေစက္ကူကို ရိုက်ထုတ်ခွင့် အခွင့်အာဏာဟာ သက်ဆိုင်ရာအာဏာပိုင်တွေထံမှာ ရှိနေပါတယ်။ အကန့်အသတ်ရယ်လို့ မရှိပါဘူး။ ငွေစက္ကူအသစ်တွေ ရိုက်ထုတ်လေ အဲ့ဒီငွေရဲ့ ဖောင်းပွနှုန်း (Inflation) ဟာ တက်လာလေပါပဲ။

ငွေဖောင်းပွတယ်ဆိုတာ လိုရင်းကတော့ ငွေရဲ့ တန်ဖိုး ကျလာတာပါပဲ။ ဥပမာ – အရင်က ငွေ (၁၀၀) ရှိရင် မုန့်ဟင်းခါးတစ်ပွဲ ဝယ်စားလို့ရပေမယ့် အခု ဝယ်စားလို့မရတော့တဲ့ သဘောမျိုးပါ။ ငွေ (၁၀၀) က မပြောင်းပေမယ့် အဲ့ဒီငွေရဲ့ ဝယ်ယူနိုင်စွမ်းအား Purchasing Power ကတော့ ငွေဖောင်းပွမှုကြောင့် ကျသွားတာပါ။ အလွန်အကျွံဖောင်းပွရင် အန္တရာယ်ရှိပေမယ့် အသင့်အတင့် ဖောင်းပွမှုကတော့ လိုအပ်တယ်လို့ ပညာရှင်များက သုတေသနပြု ဖော်ထုတ်ထားကြပါတယ်။ ငွေရဲ့တန်ဖိုးဟာ ကျုံ့ပြီး (Deflation) တန်ဖိုးတက်နေရင် လူတွေက ငွေကို မသုံးပဲ စုထားကြမှာပါ။ ငွေရဲ့တန်ဖိုး ကျနေတဲ့အခါ စုထားရင် အဲ့ဒီငွေဟာ အလိုလို တန်ဖိုးကျနေမှာ ဖြစ်တဲ့အတွက်၊ ဒါကို မလိုလားတဲ့အခါ ပိုပြီးတော့ ရင်းနှီးမြှုပ်နှံကြရပါတယ်။ ပိုပြီးတော့ သုံးကြရပါတယ်။ ဒီတော့မှာ ငွေလည်ပါတ်မှု Circulation အားကောင်းပြီး စီးပွားရေးတိုးတက်မှုနှုန်းကိုလည်း အထောက်အကူဖြစ်မှာလို့ ဆိုကြတာပါ။

ဒီတော့ အစိုးရအာဏာပိုင်တွေက မူဝါဒပိုင်းမှာ ငွေဖောင်းပွမှုနှုန်းတစ်ခု ရှိနေစေမယ့် မူဝါဒတွေ ချထားလေ့ရှိကြပါတယ်။ တစ်နှစ်ကို ပုံမှန်ငွေဖောင်းပွနှုန်းဟာ (၂%) ခန့် ဝန်းကျင်မှာ ရှိသင့်တယ်လို့ ဆိုပါတယ်။ အထက်မှာပြောခဲ့တဲ့ ၂၀၀၈ ငွေကြေးစီးပွားပျက်ကပ်ကာလမှာတော့ ထောက်ပံ့ကြေးငွေတွေ ထုတ်ပေးနိုင်ဖို့နဲ့ ချေးငွေတွေထုတ်ပေးနိုင်ဖို့အတွက်၊ ငွေစက္ကူတွေ ရိုက်ထုတ်ရတဲ့အတွက် အမေရိကန်နိုင်ငံရဲ့ ငွေဖောင်း

ပွန်းဟာ (၃.၈%) ထိရှိခဲ့ပါတယ်။ ဖြစ်သင့်တဲ့ ပမာဏထက် နှစ်ဆနီးပါး ပိုဖောင်းပွသွားတာပါ။ အခု (၂၀၂၀) ခုနှစ် ဝန်းကျင်မှာ Covid-19 ကပ်ရောဂါကာလ အလားတူ ထောက်ပံ့ကြေးငွေတွေ ထုတ်ပေးခဲ့ရပြန်လို့ (၂၀၂၁) ခုနှစ်ရဲ့ အမေရိကန်ဒေါ်လာ ငွေဖောင်းပွန်းဟာ (၅%) ထိ ရှိလိမ့်မယ်လို့ သိရပါတယ်။

လိုရင်းအနှစ်ချုပ်ကတော့ ကျွန်တော်တို့ လက်ရှိအသုံးပြုနေကြတဲ့ Fiat Money ဟာ ကြာရှည်ခံဖလှယ်ဖို့အတွက် အသုံးဝင်ပေမယ့် Store of Value ခေါ် အဖိုးတန် အရာတစ်ခုအနေနဲ့ သိမ်းဆည်းထားဖို့တော့ မသင့်တော်ဘူးလို့ ဆိုနိုင်ပါတယ်။ ငွေဖောင်းပွန်းကို ကာမိစေနိုင်တဲ့ အတိုးနှုန်းတွေဘာတွေ ရှိပေမယ့် ငွေရဲ့ Purchasing Power ကတော့ ကြာလာလေ ကျလာလေပါပဲ။ ဒါ့အပြင် ကိုယ့်ရဲ့ပိုင်ဆိုင်မှု တန်ဖိုးတွေဟာ အစိုးရရဲ့ မူဝါဒတစ်ချက်နဲ့ ဘဏ်တွေရဲ့ စွမ်းဆောင်ရည်တစ်ချက်ပေါ်မှာ မူတည်နေရတဲ့ သဘောပါ။

ဒီနေရာမှာ ဒါတွေပြောတဲ့အခါ အချက် (၃) ချက်ကို သတိပြုပေးပါ။

၁။ စာရေးသူဟာ စီးပွားရေးပညာ ဘာသာရပ်တွေကို ကျွမ်းကျင်သူမဟုတ်ပါဘူး။ အခုပြောခဲ့တဲ့အချက်အလက်တွေဟာ လေ့လာသိရှိမိသလောက် <u>သက်ဆိုင်ရာ ပညာရှင်များရဲ့ ဖော်ပြချက်တွေကို တစ်ဆင့်ပြန်ဖော်ပြခြင်းသာ</u> ဖြစ်ပါတယ်။

၂။ အခုထိ Bitcoin အကြောင်း မရောက်သေးပဲ ဒါတွေ ပြောနေရတာကတော့ Bitcoin ဟာ ငွေကြေးစနစ်တစ်မျိုးဖြစ်လို့ ဒီအခြေခံသဘောတွေကို သိရှိထားမှသာ Bitcoin ရဲ့သဘောကို နားလည်နိုင်မှာ မို့လို့ပါ။ တချို့ ငွေကြေးကဏ္ဍကို နားလည်ပြီးသား စာဖတ်သူတွေက ဒီအပိုင်းမှာ စာရေးသူထက်တောင် ပိုသိပါလိမ့်မယ်။ ဒါပေမယ့် <u>မသိတဲ့သူတွေရှိခဲ့ရင် ရှေ့ဆက်လေ့လာရတာ အထောက်အကူ ဖြစ်စေဖို့အတွက်</u> အခုလို ဖော်ပြခြင်း ဖြစ်ပါတယ်။

၃။ အခုဖော်ပြခဲ့တဲ့ အစဉ်အလာငွေကြေးစနစ်ရဲ့ အားနည်းချက်တွေဟာ စာရေးသူရဲ့ ကိုယ်ပိုင်အဆိုပြုချက်မဟုတ်ပါဘူး။ Bitcoin နဲ့ Cryptocurrency Community တွေမှာ အတွေ့ရများတဲ့ အဆိုပြုချက်တွေ ဖြစ်ပါတယ်။ <u>ဒီအဆိုပြုချက်တွေကို လက်ခံခြင်း လက်မခံခြင်းဟာ စာဖတ်သူပေါ်မှာ မူတည်ပါတယ်</u>။ အငြင်းပွားစရာ ကောင်းတဲ့ အကြောင်းအရာတစ်ခုဖြစ်လို့ ကိုယ်တိုင်သုံးသပ်ဆင်ခြင်ပြီး လက်ခံဖို့ သင့်မသင့် ဆုံးဖြတ်ရမှာပဲ ဖြစ်ပါတယ်။

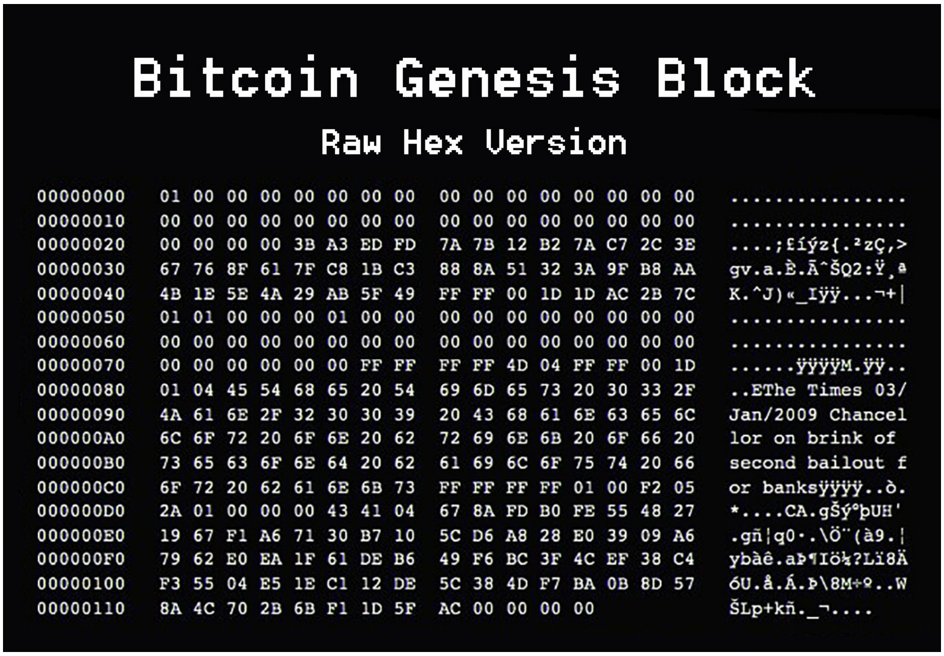
Bitcoin စတင်ခြင်း

၂၀၀၈ ခုနှစ်၊ နိုဝင်ဘာလ (၁) ရက်နေ့မှာ စတင်ဖြန့်ဝေရာကနေ ဖြစ်ပေါ်လာခဲ့တဲ့ Bitcoin ဟာ ၂၀၀၈ ငွေကြေးစီးပွားပျက်ကပ်ရဲ့ တွန်းအားပေးမှုကြောင့် ထွက်ပေါ်လာခြင်းဖြစ်ပြီး၊ ဗဟိုထိမ်းချုပ်မှုအောက် ကနေ သွားရတဲ့ ငွေကြေးစနစ်ရဲ့ အားနည်းချက်တွေကြောင့် Fiat Money ကို အစားထိုးနိုင်ဖို့ တီထွင်ခဲ့ခြင်း ဖြစ်တယ်လို့ ဆိုနိုင်ပါတယ်။

Satoshi Nakamoto ရဲ့ မူလဖြန့်ဝေချက် White Paper မှာ အဲ့ဒီလိုအတိအကျ ထည့်ပြောမထားပါဘူး။ <u>ကြားခံအဖွဲ့အစည်းမလိုဘဲ တိုက်ရိုက်ဖလှယ်နိုင်သော ဒစ်ဂျစ်တယ်ငွေကြေးစနစ်လို့သာ</u> ပြောထားပါတယ်။ Satoshi ရဲ့ ဖြန့်ဝေချက် မူရင်းအီးမေးလ်တွေကို ဒီလိပ်စာမှာ အပြည့်အစုံ လေ့လာနိုင်ပါတယ်။

https://satoshi.nakamotoinstitute.org/emails

ဒါပေမယ့် သိပ်မကြာခင်မှာ Satoshi ကိုယ်တိုင် ဖန်တီးခဲ့တဲ့ Genesis Block လို့ခေါ်တဲ့ Bitcoin ရဲ့ပထမ ဆုံး မှတ်တမ်းမှာ အခုလို Message တစ်ခု ပါဝင်ပါတယ် –



Bitcoin Genesis Block

Raw Hex Version

```
00000000  01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000020  00 00 00 00 3B A3 ED FD  7A 7B 12 B2 7A C7 2C 3E  ....;£íýz{.²zÇ,>
00000030  67 76 8F 61 7F C8 1B C3  88 8A 51 32 3A 9F B8 AA  gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040  4B 1E 5E 4A 29 AB 5F 49  FF FF 00 1D 1D AC 2B 7C  K.^J)«_Iÿÿ...¬+|
00000050  01 01 00 00 00 01 00 00  00 00 00 00 00 00 00 00  ................
00000060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000070  00 00 00 00 00 00 FF FF  FF FF 4D 04 FF FF 00 1D  ......ÿÿÿÿM.ÿÿ..
00000080  01 04 45 54 68 65 20 54  69 6D 65 73 20 30 33 2F  ..EThe Times 03/
00000090  4A 61 6E 2F 32 30 30 39  20 43 68 61 6E 63 65 6C  Jan/2009 Chancel
000000A0  6C 6F 72 20 6F 6E 20 62  72 69 6E 6B 20 6F 66 20  lor on brink of
000000B0  73 65 63 6F 6E 64 20 62  61 69 6C 6F 75 74 20 66  second bailout f
000000C0  6F 72 20 62 61 6E 6B 73  FF FF FF FF 01 00 F2 05  or banksÿÿÿÿ..ò.
000000D0  2A 01 00 00 00 43 41 04  67 8A FD B0 FE 55 48 27  *....CA.gŠý°þUH'
000000E0  19 67 F1 A6 71 30 B7 10  5C D6 A8 28 E0 39 09 A6  .gñ¦q0·.\Ö¨(à9.¦
000000F0  79 62 E0 EA 1F 61 DE B6  49 F6 BC 3F 4C EF 38 C4  ybàê.aÞ¶Iö¼?Lï8Ä
00000100  F3 55 04 E5 1E C1 12 DE  5C 38 4D F7 BA 0B 8D 57  óU.å.Á.Þ\8M÷º..W
00000110  8A 4C 70 2B 6B F1 1D 5F  AC 00 00 00 00           ŠLp+kñ._¬....
```

Bitcoin Genesis Block

ညာဘက်ခြမ်းကို ကြည့်ပါ။ The Times 03/Jan/2009 Chancellor on brink of second bailout for banks ဆိုတဲ့ Message တစ်ခုကို တွေ့ရနိုင်ပါတယ်။ အဲ့ဒါဟာ 03/Jan/2009 ရက်စွဲနဲ့ ထုတ်ဝေခဲ့တဲ့ ဗြိတိန်အခြေစိုက် The Times သတင်းစာ မျက်နှာဖုံးပါ သတင်းခေါင်းစဉ် တစ်ခုပါ။

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Francis Elliott Deputy Political Editor
Gary Duncan Economics Editor

Alistair Darling has been forced to consider a second bailout for banks as the lending drought worsens.

The Chancellor will decide within weeks whether to pump billions more into the economy as evidence mounts that the £37billion part-nationalisation last year has failed to keep credit flowing. Options include cash injections, offering banks cheaper state guarantees to raise money privately or buying up "toxic assets", The Times has learnt.

The Bank of England revealed yesterday that, despite intense pressure, the banks curbed lending in the final quarter of last year and plan even tighter restrictions in the coming months. Its findings will alarm the Treasury.

The Bank is expected to take yet more aggressive action this week by cutting the base rate from its current level of 2 per cent. Doing so would reduce the cost of borrowing but have little effect on the availability of loans.

Whitehall sources said that ministers planned to "keep the banks on the boil" but accepted that they need more help to restore lending levels. Formally, the Treasury plans to focus on state-backed gurantees to encourage private finance, but a number of interventions are on the table, including further injections of taxpayers' cash.

Under one option, a "bad bank" would be created to dispose of bad debts. The Treasury would take bad loans off the hands of troubled banks, perhaps swapping them for government bonds. The toxic assets, blamed for poisoning the financial system, would be parked in a state vehicle or "bad bank" that would manage them and attempt to dispose of them while "detoxifying" the mainstream banking system.

The idea would mirror the initial proposal by Henry Paulson, the US Treasury Secretary, to underpin the American banking system by buying

Continued on page 6, col 1
Leading article, page 2

99p
Pub chain cuts the price of a pint from £1.69 to 1989 levels
Business, page 47

The Times – 03/Jan/2009 – မျက်နှာဖုံးပုံတစ်စိတ်တစ်ပိုင်း

ဒါဟာ အစိုးရရဲ့ ဘဏ်တွေအပေါ် အကာအကွယ်ပေးရတဲ့ လုပ်ရပ်ကို ထောက်ပြခြင်းဖြစ်လို့၊ ဒီ Message ကို ကြည့်မယ်ဆိုရင် Satoshi ရဲ့ ရည်ရွယ်ချက်ကို မြင်သာစေမှာပဲ ဖြစ်ပါတယ်။

Bitcoin ဟာ Satoshi Nakamoto က စတင်တီထွင်ဖော်ထုတ်ခဲ့တဲ့ အရာလို့ ဆိုပေမယ့် Bitcoin ဖြစ်ပေါ်လာဖို့ အသုံးပြုထားတဲ့ နည်းပညာတွေက အသစ်အဆန်းတော့ မဟုတ်ပါဘူး။ ဟိုးအရင်ကတည်းက အခိုင်အမာ ရှိနေပြီးသား နည်းပညာတွေကို ပေါင်းစပ် အသုံးပြုထားတာပါ။ ဒစ်ဂျစ်တယ်ငွေကြေး ဆိုတဲ့ အိုင်ဒီယာကလည်း အသစ်အဆန်း မဟုတ်ပါဘူး။ ဥပမာ – ဗွီဒီယိုဂိမ်းတို့ အင်တာနက်ဂိမ်းတို့ထဲမှာ အသုံးပြုရတဲ့ ဒစ်ဂျစ်တယ်ငွေတွေ Point တွေကို၊ ဝါသနာရှင်အချင်းချင်း တန်ဖိုးသတ်မှတ်ပြီး အပြင်မှာ တစ်ကယ့်ငွေအစစ်နဲ့ အရောင်းအဝယ်ပြုလုပ်နေကြတာ ဟိုးအရင်ကတည်းကပါ။ ဒါပေမယ့် Satoshi ရဲ့ အိုင်ဒီယာနဲ့ နည်းပညာပေါင်းစပ်မှုက ပြည့်စုံခိုင်မာပြီး လက်တွေ့ကျတဲ့ တီထွင်မှုတစ်ခုဖြစ်သွားခဲ့တာပါ။

Satoshi Nakamoto ဘယ်သူလဲ

ဒီစာကိုရေးသားနေချိန်မှာ Bitcoin ရဲ့ ကွိုင်အရေအတွက် (၁၈) သန်းကျော်ထိ ရှိနေပြီဖြစ်ပြီး စုစုပေါင်းဈေးကွက်တန်ဖိုး Market Cap က ဒေါ်လာ (၆၀၀) ဘီလီယံကျော်ထိ ရှိနေပါပြီ။ အဲ့ဒီလောက်ထိ ကြီးကျယ်ပြီး ကမ္ဘာကို ကိုင်လှုပ်နေတဲ့ နည်းပညာကို တီထွင်ခဲ့သူ Satoshi Nakamoto ဆိုတာ ဘယ်သူလည်း တိတိကျကျ ဘယ်သူမှ မသိကြပါဘူး။

Satoshi ဟာ အလွန်လျှို့ဝှက်သူပါ။ သူ့ရဲ့ဆွေးနွေးချက်တွေမှာ နည်းပညာပိုင်းကိုပဲ အဓိကဆွေးနွေးပြီး ပုဂ္ဂိုလ်ရေးအချက်အလက်တွေ ပါဝင်လေ့မရှိပါဘူး။ သူ့ရဲ့ ပရိုဖိုင်တစ်ခုမှာ ဂျပန်နိုင်ငံမှာနေထိုင်တဲ့ အသက် (၃၇) အရွယ်ရှိသူလို့ ဖော်ပြထားပေမယ့် သူ့ရဲ့ အပြောအဆို အသုံးအနှုန်းတွေက Native-Level အင်္ဂလိပ်ဖြစ်နေလို့ ဂျပန်လူမျိုး ဖြစ်နိုင်ခြေမရှိဘူးလို့ သုံးသပ်ကြပါတယ်။ ဒါပေမယ့် Satoshi ရဲ့ အင်တာနက်လှုပ်ရှားမှုတွေဟာ ဂျပန်နိုင်ငံရဲ့ ညအိပ်ချိန်တွေမှာဆိုရင် တိတ်ဆိတ်နေလေ့ရှိလို့ အမှန်တစ်ကယ် ဂျပန်နိုင်ငံမှာ အခြေချ နေထိုင်သူ ဖြစ်နိုင်ခြေရှိတယ်လို့လည်း ဆိုကြပြန်ပါတယ်။

သူ့ရဲ့စာတွေထဲမှာ ပါဝင်တဲ့ စကားလုံးအသုံးအနှုန်းတွေကြောင့် ဗြိတိန်၊ ဩစတြေးလျ၊ ကနေဒါ စတဲ့နိုင်ငံတွေအပါအဝင် ဗြိတိလျှံနေသဟာယ နိုင်ငံတစ်ခုခုကလူ ဖြစ်ရမယ်လို့လည်း သုံးသပ်ကြပါတယ်။ တစ်ကယ့်ကို ခန့်မှန်းရခက်ပြီး လျှို့ဝှက်လွန်းသူပါ။ Satoshi Nakamoto ဖြစ်နိုင်ခြေရှိသူလို့ ခန့်မှန်းခံရသူ အများအပြားရှိပြီး၊ တစ်ကယ်လည်း မဟုတ်ဘဲနဲ့ သူဟာ Satoshi Nakamoto ပါလို့ လူရှေ့ထွက် ပြောဆိုခဲ့သူတွေလည်း ရှိနေပါတယ်။ Satoshi Nakamoto ဖြစ်နိုင်ခြေရှိသူများထဲက (၂) ဦးအကြောင်းကို ထည့်ပြောချင်ပါတယ်။

Dorian Nakamoto – အမေရိကန်၊ ကာလီဖိုးနီးယားမှာ နေထိုင်သူ Dorian Nakamoto ဆိုသူရဲ့ မွေးနာမည်ရင်းက Satoshi Nakamoto ဖြစ်ပါတယ်။ သူဟာ ရူပဗေဒဘွဲ့ရတစ်ဦးဖြစ်ပြီး၊ စစ်ဘက်ဆိုင်ရာ ပရောဂျက်တချို့မှာ ကွန်ပျူတာအင်ဂျင်နီယာတစ်ဦးအနေနဲ့ လုပ်ကိုင်ခဲ့ပြီး ငွေကြေးနည်းပညာပိုင်း ပရောဂျက်တွေလည်း ပါဝင်ပါတယ်။ ဒါကြောင့် အမည်အရရော၊ ကျွမ်းကျင်မှုအရပါ တိုက်ဆိုင်နေပါတယ်။ သတင်းထောက် တစ်ယောက်က Bitcoin အကြောင်း ရှောင်တခင် သူ့ကိုမေးတဲ့အခါ၊ သူလုပ်ခဲ့တာ ဟုတ်မှန်ကြောင်း၊ ဒါပေမယ့် အခုဆက်လက်ပါဝင်ခြင်း မရှိတော့ကြောင်း၊ အဲ့ဒီအကြောင်း ဆက်ပြောလို့မရကြောင်း၊ ပြောခဲ့လို့ ၂၀၁၄ ခုနှစ်လောက်က သတင်းတွေထဲမှာ Dorian Nakamoto ဟာ Satoshi Nakamoto ဖြစ်ပါတယ်ဆိုပြီး ပါလိုက်ပါသေးတယ်။

Dorian Nakamoto

ဒါပေမယ့် နောက်ပိုင်းမှာ သူ့ကို စစ်ဘက်ပရောဂျက် တစ်ခုအကြောင်း မေးတယ်ထင်လို့ နားလည်မှုလွဲပြီး ဖြေမိတာဖြစ်ကြောင်း၊ Bitcoin ဆိုတာ ကြားတောင် မကြားဖူးကြောင်း အကျယ်တစ်ဝင့် ပြန်ပြီးတော့ ဖြေရှင်းချက်ထုတ်ခဲ့ပါတယ်။

Hal Finney – အခု ကွယ်လွန်သွားပြီဖြစ်တဲ့ Hal Finney ဟာ PGP လို့ခေါ်တဲ့ Cryptography နည်းပညာကို တီထွင်ခဲ့သူဖြစ်လို့ Cryptography ပိုင်းမှာ အလွန်ကျွမ်းကျင်သူ တစ်ဦးပါ။ Bitcoin ကို Satoshi တီထွင်ပြီးနောက် ပထမဆုံး အသုံးပြုခဲ့သူလည်း ဖြစ်ပါတယ်။ Bitcoin ကုဒ်ကိုလည်း ပိုကောင်းအောင် ဝိုင်းကူပေးခဲ့ပါသေးတယ်။ ထူးခြားချက်ကတော့ Hal Finney ဟာ Dorian Nakamoto နဲ့ လမ်းတချို့ပဲခြားတဲ့ ရပ်ကွက်မှာ နေတဲ့သူပါ။ အင်တာနက်မှာ ကိုယ်ယောင်ဖျောက်ချင်လို့ Nakamoto အမည်ကို ယူသုံးခဲ့တာမျိုး ဖြစ်နိုင်ပါတယ်။ နောက်ထပ် ထူးခြားချက်ကတော့ Satoshi Nakamoto ပိုင်ဆိုင်တယ်လို့ ယူဆရတဲ့ Bitcoin (၁) သန်းခန့်ဟာ လှုပ်ရှားမှုမရှိဘဲ ငြိမ်နေတာ ကြာပါပြီ။ လက်ရှိပေါက်ဈေးအရ ဒေါ်လာ ဘီလီယံပေါင်းများစွာ တန်ပြီး ကမ္ဘာ့အချမ်းသာဆုံးစာရင်း ဝင်သွားနိုင်လောက်တဲ့ ပမာဏပါ။ ဒီလောက်ပမာဏရှိတဲ့ အရာတစ်ခု လုံးဝအပြောင်းအရွှေ့မရှိဘဲ ငြိမ်နေတာဟာ ပိုင်ရှင် သေဆုံးသွားလို့သာ ဖြစ်နိုင်တယ်လို့

သုံးသပ်ကြပါတယ်။ Hal Finney ဟာ ၂၀၁၄ ခုနှစ် ဩဂုတ်လမှာ ALS ရောဂါကြောင့် သေဆုံးခဲ့ရပါတယ်။

ဒီလိုမျိုး ဖြစ်နိုင်ခြေရှိတယ်လို့ ယူဆခံရသူတွေ ရှိပေမယ့် ဘယ်သူမှတော့ ခုထိ တိတိကျကျ အတည်ပြုနိုင်ခြင်း မရှိသေးပါဘူး။ လက်ရှိမှာ Satoshi Nakamoto ဟာ လုံးဝပျောက်ကွယ်နေပြီ ဖြစ်ပြီး သူဘယ်သူလဲဆိုတာ ပဟေဠိတစ်ခု ဖြစ်ကျန်နေဆဲပဲဖြစ်ပါတယ်။ တချို့ကလည်း Satoshi Nakamoto ဆိုတာ လူတစ်ဦး မဟုတ်ဘူး၊ လူတစ်ဦးအမည်ခံထားတဲ့ လျှို့ဝှက်အဖွဲ့အစည်းတစ်ခု ဖြစ်တယ်လို့ ဆိုကြပါသေးတယ်။

လက်ရှိ Bitcoin ကို ဘယ်သူထိန်းချုပ်ထားသလဲ

Satoshi Nakamoto ဟာ ၂၀၁၁ ခုနှစ်၊ ဧပြီလ (၂၆) ရက်နေ့မှာ သူ့ရဲ့ နောက်ဆုံးစာကို ပေးပို့ပြီး Bitcoin Core လို့ခေါ်တဲ့ သူကိုယ်တိုင် စတင်ရေးသားဖန်တီးခဲ့တဲ့ ပရောဂျက်ကနေ ထွက်ခွာသွားခဲ့ပြီ ဖြစ်ပါတယ်။ "လျှို့ဝှက်ဆန်းကျယ်သူတစ်ဦးက ကိုင်ထားတဲ့ ပရောဂျက် မဖြစ်စေချင်ဘူး၊ အများပိုင်းဝန်း ဖန်တီးကြတဲ့ ပရောဂျက်တစ်ခုသာ ဖြစ်စေချင်ပါတယ်" လို့ပြောပြီး Gavin Andresen ဆိုသူထံ Bitcoin Core ပရောဂျက်ကို လွှဲအပ်ခဲ့ပါတယ်။ ဒီနေရာမှာ –

၁။ Bitcoin နည်းပညာအိုင်ဒီယာ
၂။ Bitcoin Core ဆော့ဖ်ဝဲနဲ့
၃။ Bitcoin Network တို့ကို ကွဲပြားဖို့လိုပါတယ်။

Bitcoin နည်းပညာအိုင်ဒီယာဆိုတာ Satoshi ရေးသားခဲ့တဲ့ White Paper ကို ဆိုလိုတာပါ။ အဲ့ဒီနည်းပညာကို သုံးပြီး Cryptocurrency ခေါ် ဒစ်ဂျစ်တယ်ငွေကြေးစနစ်ကို မည်သူမဆို ကန့်သတ်ချက်မရှိဘဲ လွပ်လပ်စွာ ဖန်တီးလို့ ရပါတယ်။ လက်တွေ့မှာလည်း အဲ့ဒီလိုဖန်တီးထားကြတာတွေ အများကြီး ရှိနေပါတယ်။

Bitcoin Core ဆိုတာကတော့ Bitcoin အိုင်ဒီယာကို လက်တွေ့အကောင်အထည် ဖော်ထားတဲ့ ပရောဂျက်တစ်ခုပါ။ ပထမဆုံးပရောဂျက်ဖြစ်ပြီး Satoshi Nakamoto ကိုယ်တိုင် အစပြုဖန်တီးခဲ့တာပါ။ ဒီပရောဂျက်ရဲ့ Source Code ဟာ Open Source ဖြစ်တဲ့အတွက် မည်သူမဆို အသုံးပြုခွင့် ရှိယုံသာမက၊ ရေးထားတဲ့ ကုဒ်တွေကို လေ့လာစမ်းစစ်ခြင်း၊ ရယူခြင်းတို့ကို ပြုလုပ်နိုင်ပါတယ်။ နောက်တစ်မျက်နှာက လိပ်စာမှာ ကြည့်နိုင်ပါတယ်။

https://github.com/bitcoin/bitcoin

Bitcoin Network ဆိုတာကတော့ ငွေပေး ငွေယူ မှတ်တမ်းအချက်အလက်တွေကို သိမ်းဆည်းထားတဲ့ ကွန်ပျူတာကွန်ယက်တစ်ခုလို့ ဆိုနိုင်ပါတယ်။ ကွန်ပျူတာတစ်လုံး၊ လူတစ်ဦး၊ အဖွဲ့အစည်းတစ်ခု ထံမှာ သိမ်းဆည်းထားခြင်း မဟုတ်ဘဲ Bitcoin Network မှာ ပါဝင်သူ လူအများထံမှာ ဖြန့်ကျက် သိမ်းဆည်းထား တာပါ။ ဒီမှတ်တမ်းကိုလည်း လူတစ်ဦး၊ အဖွဲ့အစည်းတစ်ခုက ကိုင်ထားတာ မဟုတ်ပါဘူး။ အဲ့ဒီလို ဗဟို ချုပ်ကိုင်မှု မရှိတာကိုက Bitcoin ရဲ့ အနှစ်သာရပါ။

ဒါကြောင့် Bitcoin ကိုလူတစ်ဦးတစ်ယောက်က ထိန်းချုပ်ထားတာမျိုး မဟုတ်ပါဘူး။ အိုင်ဒီယာက လူ တိုင်းရယူနိုင်သလို၊ ပရောဂျက်ကလည်း Open Source ပါ။ အချက်အလက်တွေကလည်း ကွန်ယက်ထဲမှာ ပါဝင်သူအားလုံးက စုပေါင်းစီမံတာဖြစ်လို့ ဗဟိုထိန်းချုပ်မှုကနေ လုံးဝ ကင်းလွတ်ပါတယ်။

အဲ့ဒီလို လူတိုင်းပါဝင်လို့ ရနေတော့ လူတိုင်းက သိမ်းထားတဲ့ အချက်အလက်တွေကို ဝင်ပြီးတော့ လုပ်ချင် ရာ လုပ်လိုက်ရင် ဘယ်လိုလုပ်မလဲ။ တန်ဖိုးရှိတဲ့ ငွေကြေးတွေကို လူတိုင်းဆီမှာ သွားသိမ်းထားတာ စိတ်ချ ရပါ့မလား။ စသည်ဖြင့် အစဉ်အလာနဲ့ လုံးဝကွဲပြားသွားပြီဖြစ်လို့ ခေါင်းထဲမှာ ဘယ်လိုမှမြင်ကြည့်လို့ မရ နိုင်တော့ဘဲ နားလည်ရ အလွန်ခက်နေတဲ့ သဘောသဘာဝတစ်ခု ဖြစ်နေပါလိမ့်မယ်။ ဒီစာအုပ်ရဲ့ ရည်ရွယ်ချက်က အဲ့ဒါကို ရှင်းပြချင်တာပါ။

ဆက်လက်လေ့လာသွားကြပါမယ်။

အခန်း (၂) – Cryptography အကျဉ်း

Mobile Money တို့ Pay တို့လို အစဉ်အလာ ဒစ်ဂျစ်တယ်ငွေပေးငွေယူ စနစ်တွေဟာ ဘဏ် (သို့မဟုတ်) ငွေကြေးဝန်ဆောင်မှု အဖွဲ့အစည်းတစ်ခုခုရဲ့ ထိန်းချုပ်စီမံမှုအောက်မှာ အချက်အလက်တွေကို သိမ်းဆည်းပြီးတော့ အလုပ်လုပ်ကြတာပါ။ Bitcoin ကတော့ အဲ့ဒီလို ဗဟိုအဖွဲ့အစည်း မရှိတော့ဘဲ အများသူငါ ပါဝင်တဲ့ Network ပေါ်မှာ အချက်အလက်တွေကို ဖြန့်ကျက်သိမ်းဆည်းပြီး အလုပ်လုပ်ပါတယ်။

ဒီလို အလုပ်လုပ်တဲ့အခါမှာ အချက်အလက်တွေ လုံခြုံစိတ်ချရဖို့နဲ့ ယုံကြည်စွာ လွှဲပို့အသုံးပြုနိုင်ဖို့အတွက် Cryptography လို့ခေါ်တဲ့ ဒစ်ဂျစ်တယ်ဝှက်စာစနစ် နည်းပညာတချို့ကို ပေါင်းစပ်အသုံးပြုထားပါတယ်။ Cryptography ကို အသုံးပြုအလုပ်လုပ်လို့လည်း Cryptocurrency လို့ခေါ်တာဖြစ်ပြီး Bitcoin ရဲ့ အလုပ်လုပ်ပုံကို နားလည်ဖို့ဆိုရင် အဲ့ဒီ Cryptography နည်းပညာတွေရဲ့ အလုပ်လုပ်ပုံကို သိရှိထားဖို့လိုပါတယ်။ သိသင့်တဲ့ သဘောသဘာဝတချို့ကို ထည့်သွင်းဖော်ပြပေးချင်ပါတယ်။

Encryption

Encryption ကို လွယ်လွယ်ပြောရရင် ဝှက်စာရေးနည်းလို့ ဆိုရပါမယ်။ ကြားလူ မသိစေချင်တဲ့ စာတွေရေးတဲ့အခါ စာကို ရေးသားသူနဲ့ လက်ခံသူသာ သိရှိနိုင်မယ့် ကုဒ်တွေအသုံးပြု ရေးသားလိုက်တဲ့သဘော ပါ။

အခြေခံအကျဆုံး ဥပမာတစ်ခုအနေနဲ့ ABCD စာလုံးတွေအစား တည်နေရာတန်ဖိုး ကိန်းဂဏန်းတွေနဲ့ အစားထိုး ပေးလိုက်မယ်ဆိုပါစို့။ A ဆိုရင် 1, B ဆိုရင် 2, C ဆိုရင် 3 စသည်ဖြင့်ပါ။ ဒီတော့ စာထဲမှာ Hello လို့ရေးချင်တဲ့အခါ **8 5 9 9 15** လို့ ရေးပေးလိုက်တာမျိုးပါ။ ကြားလူက **8 5 9 9 15** ဆိုတဲ့ ဝှက်စာကုဒ်ကို တွေ့တဲ့အခါ ဘာကိုဆိုလိုမှန်း မသိပေမယ့် လက်ခံရရှိသူက အင်္ဂလိပ် စာလုံးတည်နေရာ တန်ဖိုးကို ကုဒ်

အနေနဲ့ အသုံးပြုထားမှန်း သိမယ်ဆိုရင် Decode လုပ် အဖြေရှာပြီး မူရင်းစာကို ရရှိနိုင်တဲ့ သဘောမျိုးပါ။

ဒါကတော့ လွယ်လွန်းပါတယ်။ တည်နေရာတန်ဖိုးရှာတဲ့အခါ စာပို့တဲ့ နေ့ရက်တန်ဖိုးနဲ့ ပေါင်းပြီးမှ ရှာရမယ်ဆိုတာမျိုး သတ်မှတ်လိုက်ရင် နည်းနည်းတော့ ပိုခက်သွားပါပြီ။ တနင်္လာနေ့ပို့ရင် ရတဲ့တန်ဖိုးကို ၁ နဲ့ ပေါင်းရမယ်။ အင်္ဂါနေ့ပို့ရင် ရတဲ့တန်ဖိုးကို ၂ နဲ့ ပေါင်းရမယ်ဆိုတာမျိုးပါ။ ဒါကြောင့် အင်္ဂါနေ့မှာ Hello ဆိုတဲ့စာကို ဝှက်စာအနေနဲ့ ရေးချင်ရင် **10 7 11 11 17** လို့ ရေးရမှာပါ။ ကုဒ်တွေ Crack လုပ်တယ်ဆိုတာ အဲ့ဒီလို ဖွက်ထားတဲ့ ကုဒ်ထဲက Pattern ကို ရှာပြီး အဖြေထုတ်ကြတာပါ။ အင်္ဂါနေ့မှာ ရေးတဲ့စာတွေဟာ Pattern ပုံစံတူကြတာကို သတိပြုမိသွားတာနဲ့ ကုဒ်ဖော်နည်း အဖြေကို သိသွားကြမှာပါ။

နောက်တစ်ဆင့်အနေနဲ့ ပေးပို့လိုသူနဲ့ လက်ခံသူ နှစ်ဦးထဲပဲသိတဲ့ Random ကျပန်း Key တန်ဖိုးတစ်ခုကို သုံးကြတာမျိုးလည်း ဖြစ်နိုင်ပါတယ်။ ဥပမာ 5–7–1 ဆိုတဲ့ တန်ဖိုးကို Key အနေနဲ့ထားပြီး ဒီ Key အရ 5 နဲ့ မြှောက်၊ 7 ကိုနှုတ်ပြီး၊ တစ်လုံးကျော်စီ 1 ကို ပေါင်းသွားရမယ်ဆိုပါစို့။ ဒါကြောင့် Hello ဆိုတဲ့စာကို ဝှက်စာအနေနဲ့ ရေးချင်ရင် **33 19 38 39 68** ဖြစ်သွားပါလိမ့်မယ်။

တစ်ကယ့်လက်တွေ့ တွက်ချက်မှုတွေကတော့ ဒီထက်အများကြီးပိုမိုရှုပ်ထွေးပါလိမ့်မယ်။ AES (Advanced Encryption Standard), IDEA (International Data Encryption Algorithm) စသည်ဖြင့် အယ်ဂေါ်ရစ်သမ်ပေါင်း များစွာကို သုတေသန စာတမ်းအသီးသီးနဲ့ ဖော်ထုတ်ထားကြတာတွေ ရှိပါတယ်။ ဒီနေရာမှာ အဲ့ဒီ အယ်ဂေါ်ရစ်သမ်တွေကို ထည့်သွင်းဖော်ပြမှာ မဟုတ်ပေမယ့် လိုအရင်းအချုပ်အားဖြင့် ဝှက်စာဖော်စနစ်တစ်ခုမှာပါဝင်တဲ့ အယ်ဂေါ်ရစ်သမ် နဲ့ Key ဆိုတဲ့ သဘောသဘာဝကို သိရှိထားစေလိုတာပါ။

Algorithm → မြှောက်–နှုတ်–တစ်လုံးကျော်ပေါင်း

Key → 5–7–1

အထက်က နမူနာအရ မြှောက်–နှုတ်–တစ်လုံးကျော်ပေါင်း ဆိုတဲ့ သတ်မှတ်ချက်ကို အယ်ဂေါ်ရစ်သမ်လို့ ဆိုနိုင်ပါတယ်။ ကုဒ်ပြောင်းချင်ရင်ပဲဖြစ်ဖြစ်၊ ကုဒ်ဖော်ချင်ရင်ပဲဖြစ်ဖြစ် ဒီ အယ်ဂေါ်ရစ်သမ်ကို သုံးနိုင်ပါတယ်။ ဒါပေမယ့် သုံးတဲ့ အယ်ဂေါ်ရစ်သမ် တူရင်တောင် Key မတူရင် ဖော်လို့ရမှာ မဟုတ်ပါဘူး။ ပေးထားတဲ့ နမူနာအရ Key က 5–7–1 ပါ။ ဒါကြောင့် မြှောက်–နှုတ်–တစ်လုံးကျော်ပေါင်း ဆိုတဲ့ အယ်ဂေါ်ရစ်သမ်ကို သိရင်တောင် 5–7–1 ဆိုတဲ့ Key ကို မသိရင် ဝှက်စာကို ဖော်လို့ရမှာ မဟုတ်ပါဘူး။

ဒီလိုမျိုး Key တစ်ခုကို အခြေပြုပြီး ဝှက်စာဖော်ရ ပြောင်းရတဲ့ နည်းပညာကို Symmetric Encryption လို့ ခေါ်ကြပါတယ်။ Bitcoin ကတော့ ECDSA (Elliptic Curve Digital Signature Algorithm) လို့ခေါ်တဲ့ အယ်ဂေါ်ရစ်သမ်ကို သုံးထားပါတယ်။ သူကတော့ Symmetric Encryption မဟုတ်ပါဘူး။ Public Key Encryption လို့ခေါ်တဲ့ နည်းပညာပါ။ Asymmetric Encryption လို့လည်း ခေါ်ပါတယ်။

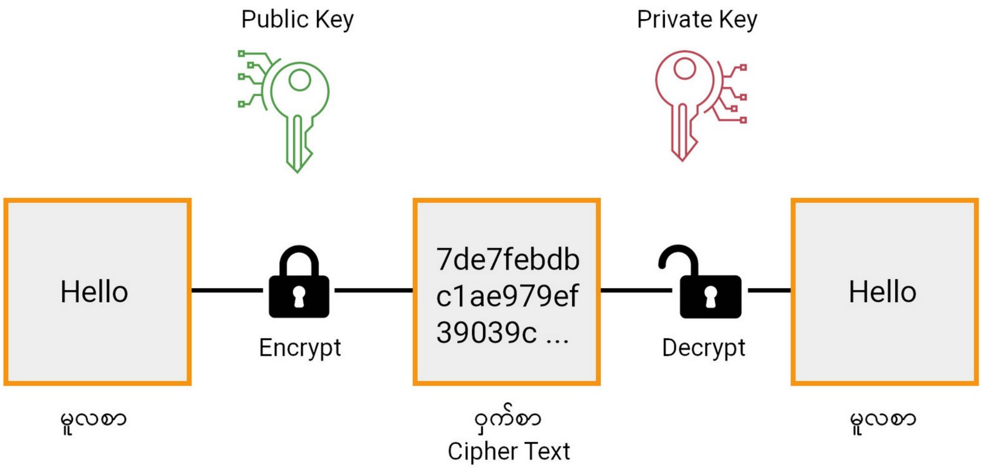
Public Key Encryption

ရိုးရိုး Symmetric Encryption ရဲ့ ပြဿနာက ပို့သူ၊ လက်ခံသူ နှစ်ဦးလုံးက Key ကို သိဖို့လိုအပ်နေခြင်း ဖြစ်ပါတယ်။ နှစ်ဦးလုံးသိတဲ့ Key တစ်ခု မရှိရင် ပို့လို့ လက်ခံလို့ မရနိုင်တော့ပါဘူး။ ဒါကြောင့် နောက်ထပ် တီထွင်မှုအနေနဲ့ ဝှက်စာရေးဖို့ Key တစ်ခု နဲ့ ဝှက်စာဖော်ဖို့ Key တစ်ခု၊ နှစ်ခုတွဲ ပါဝင်တဲ့ နည်းပညာကို တီထွင်ကြပြီး အဲ့ဒီနည်းပညာကို Public Key Encryption လို့ခေါ်တာပါ။

ဒီနည်းပညာကတော့ သော့ခလောက်တစ်ခုသာ ရှိပေမယ့် သော့တံနှစ်ခုရှိတဲ့ တံခါးလိုပါပဲ။ ထူးခြားချက် အနေနဲ့ သော့တံ A နဲ့ ခတ်လိုက်ရင် သော့တံ B နဲ့မှ ပြန်ဖွင့်လို့ရပါတယ်။ အပြန်အလှန်အားဖြင့် သော့တံ B နဲ့ ခတ်လိုက်ရင် သော့တံ A နဲ့မှ ပြန်ဖွင့်လို့ရပါတယ်။ ဒီသဘောလေးကို အတော်မျက်စိလည်သွားတတ်ကြ လို့ သေချာပြန်ကြည့်ပေးပါ။ သော့နှစ်ချောင်းရှိပြီး သော့ခတ်ချင်တဲ့အခါ ပထမတစ်ချောင်းကို သုံးရပါ တယ်။ ပြန်ဖွင့်ချင်တဲ့အခါ ဒုတိယတစ်ချောင်းကို သုံးရတာပါ။

ဒီသဘောပါပဲ၊ Public Key Encryption မှာလည်း Key နှစ်ခုရှိပြီး Public Key နဲ့ Private Key လို့ ခေါ်ကြ ပါတယ်။ Public Key ကိုသုံးပြီး ဝှက်စာဖွဲ့လိုက်ရင် Private Key နဲ့မှသာ ပြန်ဖော်လို့ရပါတယ်။

Private Key ကို ကိုယ်တိုင် လုံခြုံစွာကိုင်ဆောင်သိမ်းဆည်းရပြီး၊ Public Key ကိုတော့ အများသူငါကို ဖြန့် ဝေပေးလို့ရပါတယ်။ တစ်ယောက်ယောက်က ကိုယ့်ဆီကို စာပို့ချင်တဲ့အခါ Public Key နဲ့ ဝှက်စာဖွဲ့ပြီး ပို့ လို့ရပါတယ်။ ကြားထဲမှာ တစ်ခြားလူက အဲ့ဒီဝှက်စာကို Public Key နဲ့ ဖော်ကြည့်လို့မရပါဘူး။ ကိုယ့်ဆီ ရောက်တော့မှ ကိုယ်သိမ်းထားတဲ့ Private Key နဲ့ အဲ့ဒီဝှက်စာကို ပြန်ဖော်ရတဲ့ စနစ်ဖြစ်ပါတယ်။

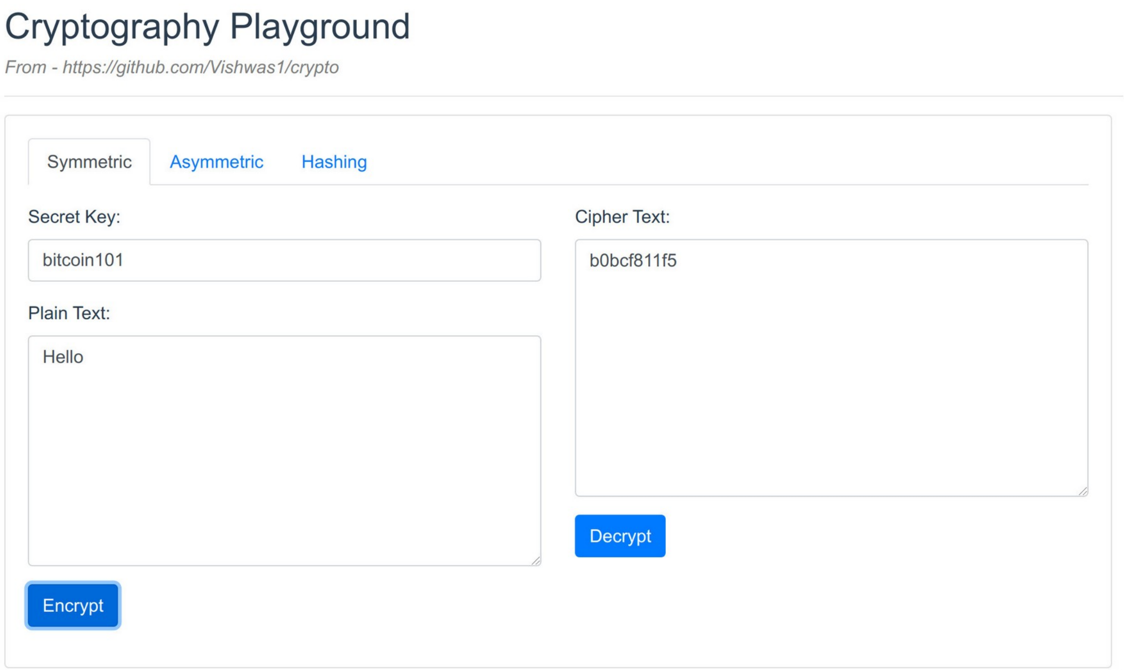


Public Key Encryption

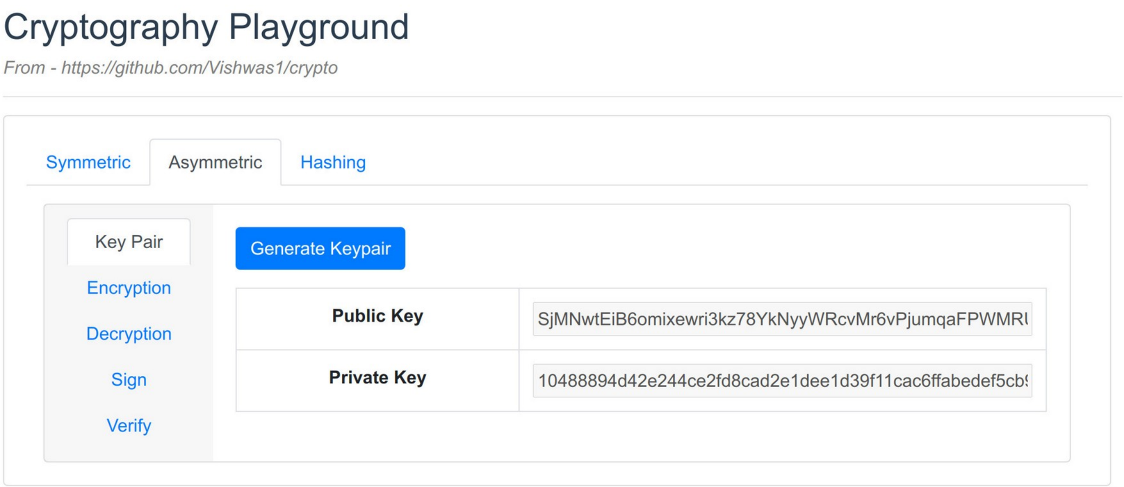
ဒီသဘောကို လက်တွေ့မျက်မြင်ကြည့်ချင်ရင် ကြည့်လို့ရအောင်လည်း စီစဉ်ထားပါတယ်။ တချို့ကိစ္စတွေက မျက်မြင်ကြည့်လိုက်မှ ပိုရှင်းတတ်လို့ပါ။ ဒီလိပ်စာမှာကြည့်ပါ။

https://eimaung.com/crypto

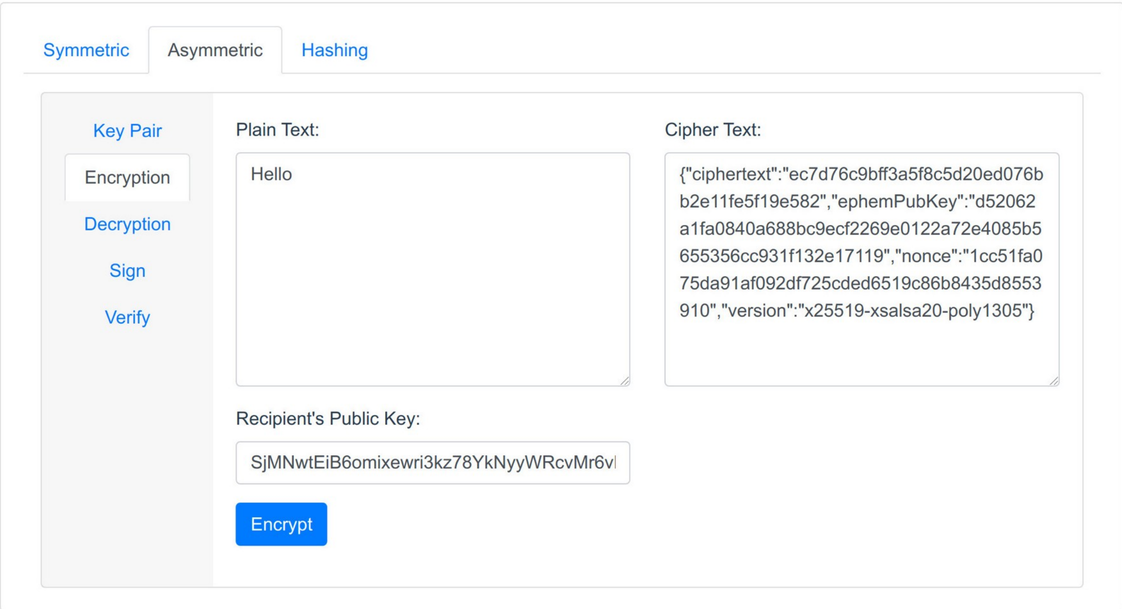
Symmetric, Asymmetric နဲ့ Hashing ဆိုပြီး (၃) ခု စမ်းစရာပေးထားပါတယ်။ Symmetric Encryption ကိုစမ်းသပ်ဖို့အတွက် Secret Key နဲ့ မူရင်းစာကိုပေးပြီး Encrypt ခလုပ်ကို နှိပ်လိုက်ရင် ဝှက်စာဖွဲ့ထားတဲ့ ကုဒ်ကို တစ်ဘက်မှာ Cipher Text အနေနဲ့ ရရှိမှာဖြစ်ပါတယ်။ မူရင်းစာနေရာမှာရော Key နေရာမှာ ကိုယ်ပေးချင်တဲ့ တန်ဖိုးအမျိုးမျိုး ပေးပြီး စမ်းကြည့်လို့ရပါတယ်။



နမူနာအရ bitcoin101 ဆိုတဲ့ Key ကိုသုံးပြီး Hello ဆိုတဲ့စာကို Encrypt လုပ်လိုက်တဲ့အခါ b0bcf811f5 ဆိုတဲ့ ဝှက်စာကို ပြန်ရပါတယ်။ နောင်အချိန်မရွေး b0bcf811f5 ကို bitcoin101 ဆိုတဲ့ Key နဲ့ Decrypt ပြန်လုပ်ရင် မူရင်းစာဖြစ်တဲ့ Hello ကိုပြန်ရမှာပါ။ Asymmetric ကိုလည်းစမ်းကြည့်နိုင်ပါတယ်။



ပထမဆုံး Generate Keypair ခလုပ်ကို နှိပ်လိုက်ရင် Private Key နဲ့ Public Key တို့ကို ထုတ်ပေးပါလိမ့်မယ်။ ကူးယူထားရပါတယ်။ ပြီးတဲ့အခါ Encryption ကိုသွားပြီး မူရင်းစာနဲ့ Public Key ကိုပေးပြီး Encrypt ခလုပ်ကို နှိပ်လိုက်ရင် ဝှက်စာဖွဲ့ထားတဲ့ ကုဒ်ကို အခုလို ရရှိမှာပါ။

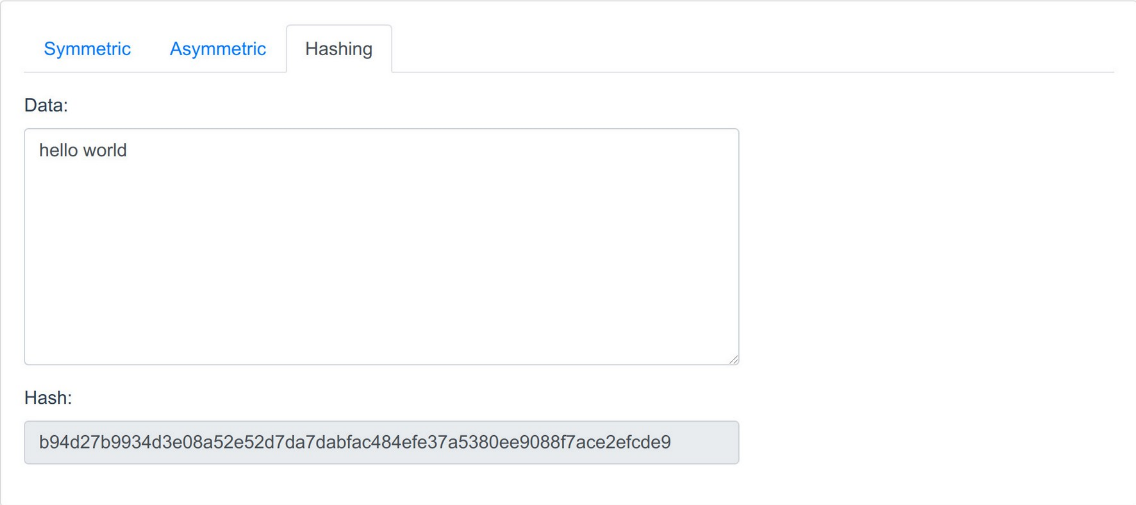


ပြီးတဲ့အခါ Decryption ကိုသွားပြီး Private Key နဲ့ ဝှက်စာကုဒ်ကို ပေးပြီး Decrypt ခလုပ်ကို နှိပ်လိုက်ရင်တော့ မူရင်းစာကို ပြန်ရမှာပါ။ ဒီနည်းနဲ့ အများကကိုယ့်ဆီကို ပို့စရာရှိရင် Public Key နဲ့ ဝှက်စာဖွဲ့ပြီးမှ ပို့လိုက်ရင် Private Key ရှိတဲ့ ကိုယ်တစ်ဦးထဲမှာ မူရင်းစာကို သိနိုင်ပါတော့တယ်။ အများက ဝှက်စာဖွဲ့ဖို့အတွက် ကိုယ့်ရဲ့ Private Key ကို သိစရာ မလိုတော့ပါဘူး။

ဒါဟာ နည်းပညာလုံခြုံရေးအတွက် အလွန်အရေးပါတဲ့ စနစ်ဖြစ်ပြီး နေရာအနှံ့အပြားမှာ အသုံးပြုကြပါတယ်။ Bitcoin ဆိုတာလည်း ဒီလို စနစ်မျိုးရှိနေလို့သာ ဖြစ်ပေါ်လာတာပါ။ နောက်ထပ် အရေးကြီးတဲ့ သဘောသဘာဝတစ်ခုဖြစ်တဲ့ Hash အကြောင်းကို ဆက်ပြောပြပါမယ်။

Hashing

လက်စနဲ့ Hashing ကို သွားပြီးတော့လည်း တစ်ခါထဲ စမ်းကြည့်သင့်ပါတယ်။ Data နေရာမှာ ကိုယ်ပေးချင်တဲ့ စာတန်ဖိုးကိုပေးလိုက်တိုင်း အောက်က Hash တန်ဖိုး လိုက်ပြောင်းနေတာကို တွေ့ရမှာပဲဖြစ်ပါတယ်။



Hash ဆိုတာဘာနဲ့တူလဲဆိုရင် ပေးလိုက်တဲ့စာကို အစိတ်စိတ်အမွှာမွှာပိုင်း၊ ရောမွှေ၊ အစိတ်စိတ်အမွှာမွှာ ထပ်ပိုင်း၊ ကျုံ့သွားအောင် ညှစ်ချ၊ အစိတ်အစိတ်အမွှာမွှာ ထပ်ပိုင်း၊ ရောမွှေပြီး နောက်ဆုံးရလဒ်ကို ပြန်ထုတ်ပေးတဲ့ သဘောမျိုးပါ။ ဒီလိုလုပ်လိုက်တဲ့အတွက် Hash Signature ကို ရလဒ်အနေနဲ့ ပြန်ရပါတယ်။ အရေးပါတဲ့ ထူးခြားချက်တချို့ကို မှတ်သားသင့်ပါတယ်။

၁။ ပေးလိုက်တဲ့ Data ပမာဏ ဘယ်လောက်ပဲဖြစ်ဖြစ် နောက်ဆုံး ပေါင်းစပ် ထုချေပြီး ထွက်လာတဲ့ <u>Hash အရွယ်အစားဟာ အတူတူပဲဖြစ်ပါတယ်</u>။ နမူနာမှာ ရလဒ် Hash ဟာ အမြဲတမ်း စာလုံး ၆၄ လုံးပဲ ပါဝင်မှာဖြစ်ပါတယ်။

၂။ ပေးလိုက်တဲ့ <u>Data တူရင် ပြန်ရတဲ့ Hash အမြဲတမ်း တူညီပါတယ်</u>။ Random သဘောမျိုး ရချင်ရာပြန်ရတာ မဟုတ်ပါဘူး။ မူရင်း Data ကို ထုချေပြီး ပြန်ရတာဖြစ်လို့ Data တူရင် ရလဒ်အမြဲတူမှာပဲ ဖြစ်ပါတယ်။ ဒီသဘောကို Digital Fingerprint လို့လည်း ခေါ်ပါတယ်။ လူတစ်ယောက်နဲ့တစ်ယောက် လက်ဗွေမတူသလို ပေးလိုက်တဲ့ Data မတူရင် ရလဒ် Hash မတူတာပါ။ ဒါပေမယ့် လက်ဗွေကိုကြည့်ပြီး ဒီလူဟုတ်မှန်ကြောင်းကိုတော့ အတည်ပြုလို့ ရပါတယ်။

၃။ ထုခြေကြေမွပြီးထွက်လာတဲ့ Hash ကို မူရင်း Data ပြန်ပြောင်းလို့ မရနိုင်တော့ပါဘူး။ ဒါဟာ Encryption ဆိုတဲ့ ဝှက်စာနဲ့ မတူတဲ့အချက်ပါ။ Encryption ဆိုတာက မူရင်းစာကို ဝှက်စာကုဒ် ပြောင်းပြီးရင် မူရင်းစာဖြစ်အောင် ပြန်ပြောင်းလို့ ရပါတယ်။ Hash ကတော့ တစ်လမ်းသွားပါ။ မူရင်းစာ Data ကို Hash ပြောင်းပြီးရင် အဲ့ဒီ Hash ကနေ မူရင်းစာ Data ကို ပြန်ပြောင်းယူလို့ မရနိုင်တော့ပါဘူး။

အိုးတစ်လုံးကို ရိုက်ခွဲလိုက်ပြီး အကွဲစတွေကနေ မူလအိုးကို ပြန်မရနိုင်သလိုပါပဲ။ ခြေတာမညက်ရင်၊ မွှေတာမနှံ့ရင်တော့ အကွဲစကို ကြည့်ပြီး မြေအိုးလား၊ ကြွေအိုးလား၊ စဉ့်အိုးလား ခန့်မှန်းလို့ရနိုင်တာမျိုးပဲ ရှိပါတယ်။ ခြေတာညက်ပြီး မွှေတာနှံ့ရင်တော့ အဲ့ဒီလိုတောင် ပြန်ခန့်မှန်းလို့ရမှာ မဟုတ်ပါဘူး။ အချက်အလက် လုံခြုံရေးအရ ခန့်မှန်းလို့ မရနိုင်တာမျိုးကို လိုချင်ကြတာပါ။ လက်ဗွေကို ကြည့်ပြီး ဒီလူဟုတ်မှန်ကြောင်း အတည်ပြုနိုင်ပေမယ့် လက်ဗွေကို ကြည့်ပြီး အသားဖြူသလား၊ မဲသလား၊ အရပ်ပုသလား၊ ရှည်သလား မသိနိုင်သလိုမျိုးပါပဲ။ အတော်လေး စိတ်ဝင်စားဖို့ကောင်းတဲ့ နည်းပညာတွေပါ။

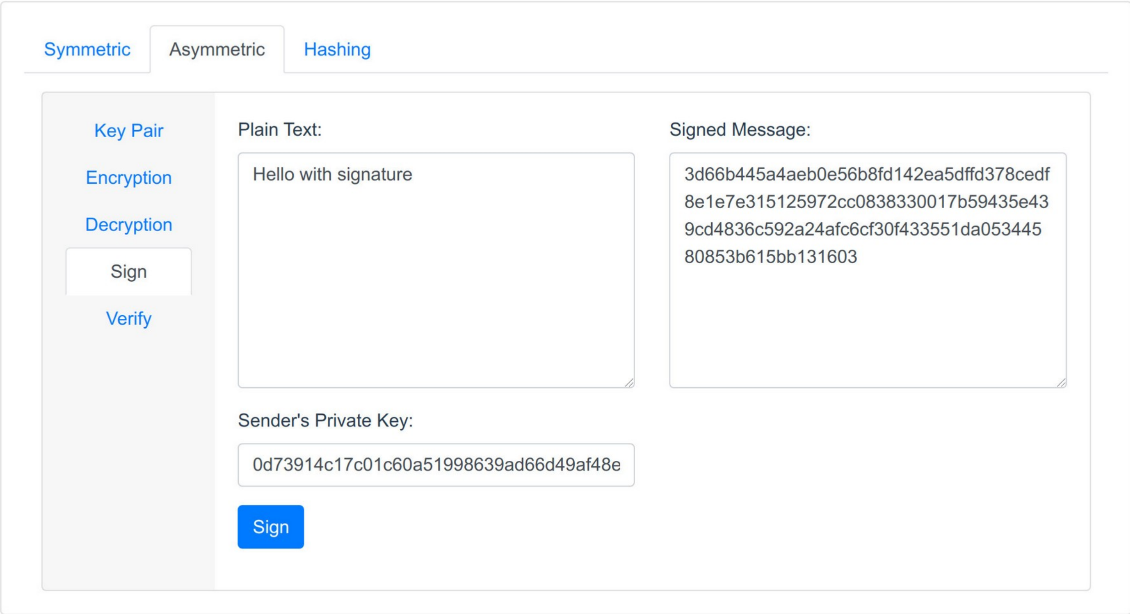
Encryption နဲ့ Hash ကို တွဲပြီး Digital Signature အနေနဲ့လည်း အသုံးပြုနိုင်ပါသေးတယ်။

Digital Signature

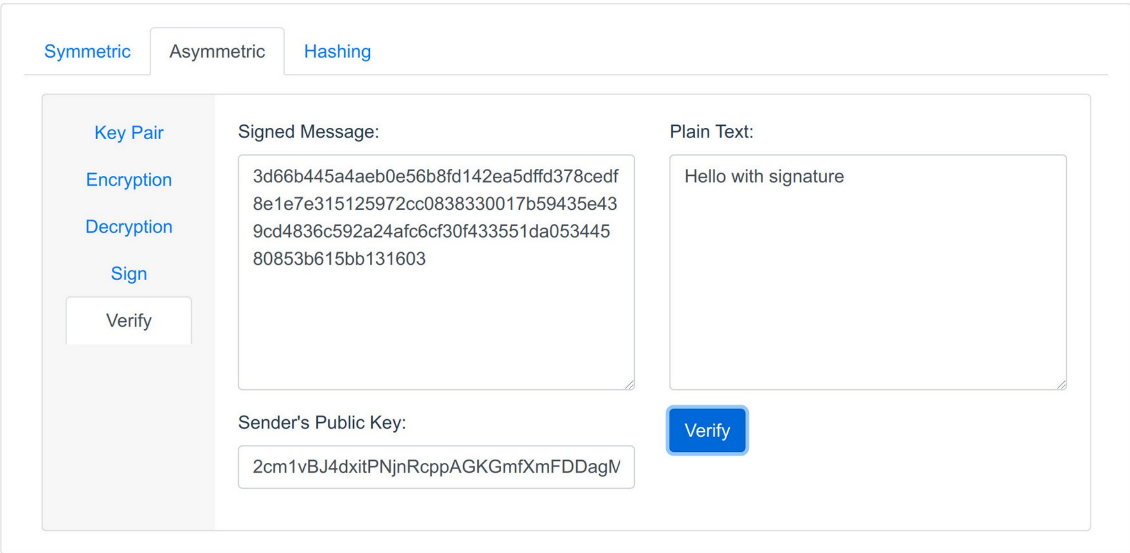
ပြင်ပမှာ စာပေးစာယူလုပ်တဲ့အခါ၊ စာချုပ်စာတမ်းတွေ ချုပ်ကြတဲ့အခါ အောက်ခြေမှာ လက်မှတ်ထိုးပြီး အတည်ပြုကြပါတယ်။ လက်မှတ်ကိုကြည့်ပြီး ဒီလူကိုယ်တိုင် ရေးတဲ့စာ၊ ဒီလိုကိုယ်တိုင် ချုပ်တဲ့စာချုပ် ဆိုတာမျိုးကို အတည်ပြုကြတာပါ။ ဒစ်ဂျစ်တယ်စနစ်နဲ့ ပေးပို့တဲ့စာတွေမှာလည်း အဲ့ဒီလို လက်မှတ်ထိုးလို့ ရနိုင်ပါတယ်။ Private Key နဲ့ ထိုးရတာပါ။

ရေးလိုက်တဲ့စာကို Private Key နဲ့ Encrypt လုပ်ပြီး မူရင်းစာနဲ့ Encrypt လုပ်ထားတဲ့ ဝှက်စာကို တွဲပို့ရတာပါ။ ဒီနည်းက ပို့တဲ့စာကို လူမသိအောင် ဝှက်ချင်တာ မဟုတ်ပါဘူး။ ပို့တဲ့စာဟာ မူလရေးသားသူကိုယ်တိုင်ပေးပို့တာ ဟုတ်မဟုတ်နဲ့၊ မူလပေးပို့ချက်အတိုင်း အတိအကျ ဟုတ်မဟုတ် ပဲ စစ်ချင်တာပါ။

လက်ခံရရှိသူက Public Key ကိုသုံးပြီး မူရင်းစာနဲ့ ဝှက်စာကိုယှဉ်ပြီး တိကျမှန်ကန်မှု ရှိမရှိ ပြန်စစ်လို့ရနိုင်ပါတယ်။



နမူနာမှာ Hello with signature ဆိုတဲ့စာကို **Private** Key နဲ့ Sign လုပ်လိုက်တဲ့အခါ တစ်ဘက်မှာ Signed Message ဆိုပြီး ဝှက်စာတစ်ခု ထွက်လာတာကို တွေ့ရနိုင်ပါတယ်။



နောက်တစ်ဆင့်မှာ Verify လုပ်ဖို့အတွက် Signed Message ရယ်၊ မူရင်းစာရယ်၊ **Public** Key ရယ် အစုံ ပေးလိုက်တဲ့အခါ မှန်ကန်မှု ရှိမရှိဆို စစ်ဆေးပေးသွားမှာ ဖြစ်ပါတယ်။

ဒီနည်းနဲ့ ဒစ်ဂျစ်တယ် စာပေးစာယူ၊ စာရွက်စာတမ်းတွေကို လက်မှတ်ထိုးရတာပါ။ Private Key နဲ့ လက်မှတ်ထိုးပြီး Public Key နဲ့ မှန်ကန်မှုရှိမရှိ ပြန်စစ်တာပါ။ ဒီ အလုပ်တွေကို ကိုယ်တိုင် အစအဆုံးလုပ်စရာမလိုပါဘူး။ အခုက မြင်သာစေချင်လို့သာ နမူနာပြထားတာပါ။ လက်တွေ့မှာ သက်ဆိုင်ရာ ဆော့ဖ်ဝဲက လုပ်ပေးသွားမှာမို့လို့ ကိုယ်ဘက်က ခလုပ်တစ်ချက်နှိပ်ယုံနဲ့ လက်မှတ်ထိုးလို့ ရနိုင်ပါတယ်။

ဒီထက်ပိုပြီး ကျယ်ကျယ်ပြန့်ပြန့်လေ့လာလိုရင် Digital Certificate တို့ Certification Authority တို့လို ကိစ္စမျိုးတွေထိ ပါဝင်တဲ့ PKI ခေါ် Public Key Infrastructure ဆိုတဲ့ အကြောင်းအရာ ဘာသာရပ်ကို လေ့လာကြရမှာပါ။ Bitcoin ရဲ့အလုပ်လုပ်ပုံ နားလည်ဖို့အတွက် အဲ့လောက်ထိ မလိုသေးပါဘူး။ Public Key Encryption နဲ့ Hash အကြောင်းကို သိရင်ပဲ ရှေ့ဆက်လေ့လာလို့ ရသွားပါပြီ။

ဒီအတိုင်းဖတ်ကြည့်တာ နည်းနည်းမျက်စိလည်နေရင် ကိုယ်တိုင် လက်တွေ့စမ်းကြည့်ဖို့ တိုက်တွန်းပါတယ်။ လက်တွေ့ကြည့်လိုက်မှ ပိုပြီးတော့ ရှင်းသွားနိုင်တဲ့အတွက်ကြောင့်ပါ။

https://eimaung.com/crypto

Consensus Algorithms

ကိုယ်မသိတဲ့ လူစိမ်းတစ်ယောက်ဆီက အရေးကြီးတဲ့ အချက်အလက်တစ်ခုကို လက်ခံရရှိတဲ့အခါ အဲ့ဒီ အချက်အလက် မှန်ကန်မှုရှိမရှိ ဘယ်လိုဆုံးဖြတ်ကြမလဲ။ ဒါ စဉ်းစားစရာပါ။ မျက်စိမှိတ် ယုံလိုက်လို့တော့ မရပါဘူး။ ပြင်ပမှာဆိုရင်တော့ အဲ့ဒီလူဘယ်သူလဲ လိုက်စုံစမ်းရတာတွေ၊ သူပေးတဲ့ အချက်အလက်ကို ကျွမ်းကျင်သူနဲ့ ပြပြီး စိစစ်ရတာမျိုးတွေ လုပ်ဖို့ လိုနိုင်ပါတယ်။

ကွန်ပျူတာ စနစ်မှာတော့ အဲ့ဒီလို ကိုယ်မသိတဲ့သူ၊ ကိုယ်မသိတဲ့နေရာကနေ လာတဲ့ အချက်အလက်တွေ မှန်ကန်မှု ရှိမရှိ ဆုံးဖြတ်ဖို့အတွက် Consensus Algorithm တွေကို အသုံးပြုကြပါတယ်။ Proof of Work, Proof of Stake, Proof of Authority, Proof of History, Proof of Capacity စသည်ဖြင့် အမျိုးမျိုးရှိပါတယ်။ ဒီသဘောတွေထဲက တချို့ကို သူ့နေရာနဲ့သူ ဆက်လက်ဖော်ပြမှာမို့လို့ ဒီနေရာမှာတော့ အကျဉ်းချုပ်ပဲ ပြောပါမယ်။

Proof of Work ဆိုတာဟာ ခက်ခဲတဲ့အလုပ်ကို လုပ်ခိုင်းပြီး၊ လုပ်ပြနိုင်တယ်ဆိုရင် သူပေးတဲ့အချက်အလက်ကို ယုံကြည်ရတယ်လို့ လိုက်ခံလိုက်တဲ့ သဘောပါ။ သင်္ချာပညာရှင် တစ်ယောက်ပါဆိုပြီး သင်္ချာပညာနဲ့ပက်သက်တဲ့ အချက်အလက်တစ်ခု တင်ပြလာသူကို တစ်ကယ်ဟုတ်မဟုတ် စိစစ်ဖို့အတွက် ခက်ခဲတဲ့ ပုဒ်စာတစ်ပုဒ်ကို လက်တွေ့တွက်ပြခိုင်းလိုက်တဲ့ သဘောမျိုးပါ။ တွက်ချက်ပြနိုင်တယ်ဆိုမှ သူတင်ပြတဲ့ အချက်အလက်ကို ဟုတ်မှန်တယ်လို့ လက်ခံလိုက်မှာပါ။

Proof of Stake ဆိုတာကတော့ ပိုင်ဆိုင်မှုကို သက်သေပြခိုင်းပြီး ပြနိုင်တယ်ဆိုရင် ယုံကြည်လက်ခံလိုက်တဲ့သဘောမျိုးပါ။ စာအုပ်အငှားဆိုင်တစ်ဆိုင်က ငွေစပေါ် ပေးထားမယ်ဆိုရင် သူမသိတဲ့ လူစိမ်းကိုလည်း စာအုပ်တွေ စိတ်ချလက်ချ ငှားပေးလိုက်လို့ ရပါတယ်။ စာအုပ်ပြန်လာမအပ်ခဲ့ရင် စပေါ်ငွေကို သိမ်းယူလိုက်လို့ ရတဲ့အတွက်ကြောင့်ပါ။ Proof of Stake ကလည်း အဲ့ဒီလိုပါပဲ။ ပိုင်ဆိုင်မှုတစ်ခုကို အာမခံထားတဲ့အခါ သူပြောတဲ့အချက်အလက် ဟုတ်မှန်ကြောင်း လက်ခံလိုက်တဲ့ သဘောမျိုးပါ။

Proof of History ဆိုတာကတော့ အရင်က အမှန်တစ်ကယ်ဖြစ်ပျက်ခဲ့ကြောင်း သက်သေပြနိုင်ရင် သူပြောတဲ့ အချက်အလက်ကို လက်ခံလိုက်တဲ့ သဘောမျိုးပါ။ လူစိမ်းတစ်ယောက်နဲ့ စကားပြောရင်း သူနဲ့ကိုယ်နဲ့ ငယ်ငယ်က တက်ခဲ့တဲ့ကျောင်း တူတယ်လို့ ဆိုလာခဲ့ရင် အပြောသက်သက်နဲ့တော့ ယုံလို့မရပါဘူး။ ဒါပေမယ့် အဲ့ဒီကျောင်းကို တစ်ကယ်တက်ခဲ့သူမှသာ သိနိုင်တဲ့အချက်အလက်ကို ပြောပြခဲ့ရင်တော့ သူပြောတာ ဟုတ်မှန်ကြောင်း လက်ခံ အတည်ယူလိုက်နိုင်တဲ့ သဘောမျိုးပါ။

ဒီလိုမျိုး ကိုယ်မသိတဲ့သူ၊ ကိုယ်မသိတဲ့နေရာက လာတဲ့အချက်အလက်တွေ မှန်ကန်မှုရှိမရှိ စိစစ်ဖို့ လိုအပ်တဲ့အတွက်၊ Bitcoin ကို ဒီဇိုင်းလုပ်တဲ့အခါ Satoshi Nakamoto က Proof of Work လို့ခေါ်တဲ့နည်းကို ရွေးချယ် အသုံးပြုခဲ့ပါတယ်။ ဒီနည်းမှာ၊ အချက်အလက်ပေးလိုသူဟာ အလွန့်အလွန် ခက်ခဲတဲ့ အလုပ်ကို လုပ်ပြဖို့အတွက် အချိန်၊ စွမ်းအင်နဲ့ လုပ်အားတွေ စိုက်ထုတ်ရတဲ့အတွက်၊ မသမာတဲ့ အချက်အလက်ကို အလွယ်တစ်ကူပေးပြီး အနှောက်အယှက်ပြုလို့ မရတော့ပါဘူး။ မသမာမှု ပေါ်သွားတဲ့အခါမှာ သူ့ဘက်က အဆမတန် စိုက်ထုတ်ခဲ့ရတဲ့ စွမ်းအင်နဲ့လုပ်အားတွေကို အကျိုးမဲ့ ဆုံးရှုံးရတော့မှာမို့လို့ပါ။

ဒီသဘောသဘာဝတွေကို ကြိုတင်သိရှိထားခြင်းဟာ Bitcoin ရဲ့အလုပ်လုပ်ပုံကို နားလည်စေဖို့အတွက် အများကြီး အထောက်အကူဖြစ်တယ် ဆိုတာကို ရှေ့ဆက်လေ့လာတဲ့အခါ တွေ့မြင်ကြရမှာပဲ ဖြစ်ပါတယ်။

အခန်း (၃) – Bitcoin အလုပ်လုပ်ပုံ

Bitcoin ဆိုတာဘာလဲ တစ်ခွန်းထဲဖြေပါဆိုရင်၊ **Distributed Ledger** ပါလို့ ဖြေနိုင်ပါတယ်။

ဥပမာ – ကိုကို၊ ဘိုဘို နဲ့ နီနီ ဆိုတဲ့ မောင်နှမ (၃) ယောက် ရှိတယ် ဆိုကြပါစို့။ ဖေဖေက ကိုကို၊ ဘိုဘို နဲ့ နီနီ တို့ကို တစ်ယောက် ငွေ (၁၀၀) စီ ပေးထားတယ်။ နောက်နေ့မှာ ဘိုဘို က နီနီ ဆီက (၂၀) ချေးတယ်၊ ကိုကို က နီနီ ကို မုန့်ဖိုး (၅၀) ပေးတယ် – စသည်ဖြင့် အပေးအယူမှတ်တမ်းတွေ ရှိလာတဲ့အခါ မေ့ပျောက်သွားမှာစိုးလို့ Ledger စာရင်းတစ်ခုအနေနဲ့ မှတ်သားထားတယ် ဆိုကြပါစို့။

အဲ့ဒီ Ledger စာရင်းကို တစ်ယောက်ထဲက ကိုင်ထားတာမျိုးမဟုတ်ဘဲနဲ့ ပုံစံတူ (၃) ခုကို (၃) ယောက်စလုံးက ကိုင်ထားတဲ့သဘောကို Distributed Ledger လို့ ခေါ်တာပါ။ ဒီလိုပုံစံတူ ကူးယူပြီး ကိုင်ထားတဲ့အတွက်၊ တစ်ယောက်က သူ့သဘောနဲ့သူ ထပ်တိုးလို့ မရတော့ပါဘူး။ ထပ်တိုးလိုက်ရင် ကျန်နှစ်ယောက်ဆီက စာရင်းနဲ့ မတူတော့တဲ့အတွက် ကျန်နှစ်ယောက်က လက်ခံမှာမဟုတ်ပါဘူး။ ဒါကြောင့် ထပ်တိုးစရာရှိရင် (၃) ယောက်စလုံးက သဘောတူမှသာ ထပ်တိုးလို့ရပြီး စာရင်း (၃) ခုစလုံးမှာ ပုံစံတူ တိုးရမှာပါ။ ဒီနည်းနဲ့ မသမာမှု ကင်းရှင်းတဲ့ စာရင်းကို ရရှိသွားခြင်း ဖြစ်ပါတယ်။

ဒီနေရာမှာ သတိပြုရမှာက – အဲ့ဒီ Ledger စာရင်းဟာ အပေးအယူမှတ်တမ်းကိုသာ သိမ်းထားတာပါ။ ကိုကို့မှာ စုစုပေါင်း ငွေဘယ်လောက်ရှိသလဲ၊ နီနီမှာ စုစုပေါင်း လက်ကျန် ငွေဘယ်လောက်ရှိသလဲ စသည်ဖြင့် Balance လို အချက်အလက်တွေကို ထည့်သိမ်းမထားပါဘူး။ ဒါကြောင့်၊ အပေးအယူမှတ်တမ်းတစ်ခု ထည့်တော့မယ်ဆိုရင် တစ်ကယ်ရော အပေးအယူလုပ်ချင်တဲ့ ငွေရှိရဲ့လား ဆိုတာကို အရင်အပေးအယူ မှတ်တမ်းတွေမှာ ပြန်ရှာပြီးစစ်ရပါတယ်။ ဥပမာ – ကိုကိုက ဘိုဘို ကို မုန့်ဖိုး (၅၀) ပေးတယ်ဆိုရင် ကိုကို့ဆီမှာ (၅၀) တစ်ကယ်ရှိသေးလို့လားဆိုတာ စာရင်းထဲမှာ အရင်ပြန်ရှာစစ်ပြီး ရှိတယ်ဆိုမှပဲ ထည့်ရမှာပါ။ ဒီလိုပြန်ရှာ

တွက်ချက်တဲ့ အလုပ်ဟာ မလွယ်ပါဘူး။ ဒါကြောင့် အဲ့ဒီလို ပြန်ရှာတွက်ပြီး စာရင်းသွင်းပေးတဲ့သူကို ဖေဖေက တစ်ခါတွက်ရင် (၁) ကျပ် ဆုချပါတယ်။ စာရင်းသွင်းခ ရတဲ့သဘောမျိုးပါ။

မသမာတဲ့နည်းနဲ့ ပြင်ချင်ရင် စာရင်းတစ်ခုထဲကို ပြင်လို့မရပါဘူး။ (၃) ခုလုံးကို ပြင်ရပါမယ်။ ဒါကြောင့် တစ်ညမှာ တစ်ယောက်က စာရင်း (၃) ခုစလုံးကို ခိုးယူပြီး ပြင်ဆင်ဖို့ကြိုးစားပါတယ်။ ဒါပေမယ့် မရပါဘူး။ ဘာကြောင့်လဲဆိုတော့ စာရင်းရေးသွင်းတုံးက Permanent Marker ကိုသုံးပြီး ရေးသွားထားလို့ ပြန်ဖျက်လို့ မရနိုင်တော့လို့ပါ။ လက်ရှိစာရင်းစာရွက်တွေကို ဖြဲထုတ်ပြီး အသစ်ထပ်ရေးထည့်ရင်လည်း ကြည့်လိုက်တာနဲ့ မမှန်ကန်တော့မှန်း သိသာနေမှာပဲ ဖြစ်ပါတယ်။

ဒါက စာရင်းစာအုပ်မှာ ရေးသွင်းတဲ့စာရင်းမို့လို့ပါ။ ဒစ်ဂျစ်တယ်ဒေတာအနေနဲ့ ရေးသွင်းတဲ့ စာရင်းမှာတော့ ဒီလိုမျိုး ပြန်ပြင်လို့ဖျက်လို့ မရနိုင်တဲ့သဘောမျိုးကို ရရှိဖို့အတွက် Blockchain လို့ခေါ်တဲ့ နည်းပညာကို အသုံးပြုကြပါတယ်။

Blockchain

Blockchain ဆိုတာ ကြားဖြတ်ပြင်ဆင်လို့ မရအောင် ရှေ့နောက်ချိတ်ဆက်တဲ့နည်းနဲ့ မှတ်တမ်းတင်တဲ့ စာရင်းတစ်မျိုးပါ။ သူ့ချည်းသက်သက်ဆိုရင် ရှုပ်ထွေးမှုမရှိလှပါဘူး။ နားလည်ရလွယ်ပါတယ်။ အရိုးရှင်းဆုံး Blockchain တစ်ခုရဲ့ဖွဲ့စည်းပုံက အခုလိုပုံစံမျိုးပဲ ဖြစ်ပါတယ်။

Genesis Block →	Block #1 →	Block #2 →	Block #3 →
Data Dad pays Ko Ko, Bo Bo & Ni Ni 100 each	Data Bo Bo borrows 20 from Ni Ni	Data Ko Ko pays 50 to Ni Ni	Data Bo Bo buys a game for 120
Previous Hash 0000000	Previous Hash 95cc830	Previous Hash d789979	Previous Hash 2b72935
Hash 95cc830	Hash d789979	Hash 2b72935	Hash 9f79124

Block တစ်ခုမှာ Data, Previous Hash နဲ့ Hash ဆိုပြီး အကြောင်းအရာ (၃) ခုစီ ပါဝင်ပါတယ်။ ပထမဆုံး Block ကို Genesis Block လို့ခေါ်ပါတယ်။ အဲ့ဒီ Genesis Block အတွက် Previous Hash မရှိပါဘူး။ သူ့

ရှေ့မှာ ချိတ်ဆက်စရာ Block မရှိသေးလို့ပါ။ Data နေရာမှာ သိမ်းချင်တဲ့အချက်အလက်ကို ထည့်သွင်းရပြီး Hash ကတော့ အဲ့ဒီအချက်အလက်ကို Previous Hash နဲ့တွဲပြီး ထုတ်ယူထားတာပါ။ ဒီလိုပါ –

```
hash( data + previous hash) → 95cc830
```

ပြီးခဲ့တဲ့စာမျက်နှာပါပေးထားတဲ့ နမူနာကို သတိပြုကြည့်ပါ။ နောက် Block ဖြစ်တဲ့ Block #1 အတွက် Previous Hash ဟာ Genesis Block ရဲ့ Hash နဲ့ တူညီနေတာကို တွေ့ရနိုင်ပါတယ်။ Block #1 က Genesis Block နဲ့ ချိတ်လိုက်တဲ့သဘောပါ။ Block #1 ရဲ့ Hash တန်ဖိုးက သူ့ Data နဲ့ Previous Hash ကို တွဲပြီးထုတ်ယူထားတာပါ။ ဆက်လက်ပြီး Block #2 အတွက် Previous Hash ဟာ Block #1 ရဲ့ Hash နဲ့ တူညီတာကို တွေ့ရမှာ ဖြစ်ပါတယ်။ ဒီနည်းနဲ့ Block တွေ တစ်ခုပြီးတစ်ခု ချိတ်ပြီးတော့ သိမ်းသွားတာပါ။

အဲ့ဒီလို ချိတ်ပြီး သိမ်းသွားတဲ့အတွက် ကြားထဲက တစ်ခုခုကို ပြင်လိုက်တာနဲ့ ချိတ်ထားတဲ့ Block အတွဲ လိုက်ဟာအချိတ်အဆက် မမိတော့ဘဲ Invalid ဖြစ်သွားမှာပါ။

Genesis Block →	Block #1 →	Block #2 →	Block #3 →
Data Dad pays Ko Ko, Bo Bo & Ni Ni 100 each	Data Bo Bo borrows 200 from Ni Ni	Data Ko Ko pays 50 to Ni Ni	Data Bo Bo buys a game for 120
Previous Hash 0000000	Previous Hash 95cc830	Previous Hash d789979	Previous Hash 2b72935
Hash 95cc830	Hash d789979	Hash 2b72935	Hash 9f79124

နမူနာမှာ Block #1 ရဲ့ Data ကို ပြင်လိုက်တဲ့အတွက် Hash တန်ဖိုး မကိုက်တော့ပါဘူး။ လွဲနေပါပြီ။ အဲ့ဒါကို မှန်အောင် ပြင်လိုက်ရင် သူ့နောက်က ချိတ်ထားတဲ့ Block #2 မှာ ရဲ့ Previous Hash နဲ့ မကိုက်တော့ပါဘူး။ အဲ့ဒါကို ဆက်ပြင်လိုက်ရင် သူ့နောက်က ဆက်ချိတ်ထားတဲ့ Block #3 နဲ့ ကိုက်တော့မှာ မဟုတ်ပါဘူး။ ဒါကြောင့် ကြားထဲက တစ်ခုကို ပြင်လိုက်တာနဲ့ နောက်ဆက်တွဲ အကုန်အချိတ်အဆက် မမိတော့ဘဲ Invalid ဖြစ်သွားတော့မှာပါ။ ဒီနည်းနဲ့ ကြားဖြတ်ပြင်ဆင်လို့မရနိုင်အောင် စီစဉ်ထားတာပါ။

ဒီနေရာမှာ မေးစရာတချို့တော့ ရှိလာနိုင်ပါတယ်။

၁။ ကြားဖြတ်မပြင်ဘဲ နောက်ဆုံးတစ်ခုနှစ်ခုပဲ ပြင်သွားရင် ဘယ်လိုလုပ်မလဲ။
၂။ ကြားဖြတ်ပြင်တဲ့အပြင် ပြင်လိုက်လို့ နောက်ဆက်တွဲ Invalid ဖြစ်သွားတဲ Block တွေကိုပါ တစ်ခုမကျန် အကုန်ပြင်သွားရင်ရော ဘယ်လိုလုပ်မလဲ။

အဲ့ဒီမေးခွန်းတွေနဲ့ ပက်သက်တဲ့အဖြေကိုရဖို့ နောက်ထပ်လုပ်ဆောင်ချက်တွေကို ဆက်ပြောသွားပါမယ်။

Proof of Work

Blockchain ထဲမှာ Block အသစ်တစ်ခုကို ထည့်သွင်းသိမ်းဆည်းတော့မယ်ဆိုရင် လိုက်နာရမယ့်အချက်တွေ ရှိပါတယ်။ ပထမတစ်ချက်ကတော့ ထည့်သွင်းလိုတဲ့အချက်အလက်ဟာ မှန်ကန်ကြောင်း စစ်ဆေးအတည်ပြုနိုင်ရပါမယ်။

နမူနာပေးထားတဲ့ Blockchain ရဲ့ Block Data နေရာမှာ ငွေပေးငွေယူမှတ်တမ်း Transaction ကို ထည့်ပြထားခဲ့ပါတယ်။ လက်တွေ့မှာ Block Data နေရာမှာ သိမ်းဆည်းလိုတဲ့ မည်သည့် အချက်အလက် အမျိုးအစားကိုမဆို သိမ်းဆည်းလို့ ရပါတယ်။ ငွေပေးငွေယူမှတ်တမ်း Transaction ကို သိမ်းမယ်ဆိုရင်လည်း Transaction တစ်ကြောင်းကို Block တစ်ခုဖြစ်စရာမလိုပါဘူး။ Block တစ်ခုထဲမှာပဲ Transaction လေးငါးဆယ်ကြောင်း၊ အကြောင်းတစ်ရာ၊ စုစည်းထည့်သွင်း သိမ်းဆည်းလို့ရပါတယ်။

နမူနာမှာ ငွေပေးငွေယူ Transaction တွေကို သိမ်းဆည်းပြခဲ့တဲ့အခါ ဘယ်သူ့မှာ ငွေလက်ကျန်ပမာဏ ဘယ်လောက်ရှိတယ်ဆိုတဲ့ အချက်ကို ထည့်သိမ်းမထားတာကို သတိပြုပါ။ Bitcoin ကလည်း အဲ့ဒီလိုပဲ ဘယ်သူ့မှာ လက်ကျန်ဘယ်လောက်ရှိသလဲဆိုတာ ထည့်မသိမ်းပါဘူး။ လက်ကျန်သိချင်ရင် ရှိထားတဲ့ ငွေပေးငွေယူမှတ်တမ်းကနေ တွက်ယူရမှာပါ။

ဥပမာ – ကိုကိုက ဘိုဘိုကို ၃၀ ပေးတယ်ဆိုတဲ့ Block အသစ်တစ်ခုထည့်ချင်တဲ့အခါ ကိုကို့မှာ အမှန်တစ်ကယ်ပေးစရာ ငွေလက်ကျန် (၃၀) ရှိရဲ့လားဆိုတာ သိဖို့လိုလာပါတယ်။ ဒါကြောင့် တွက်ကြည့်လိုက်တဲ့အခါ –

၁။ ကိုကို့ ကို ဖေဖေက ၁၀၀ ပေးခဲ့တယ်။
၂။ ကိုကို က နီနီကို ၅၀ ပေးခဲ့တယ်။
၃။ ဒါကြောင့် ကိုကိုမှာ လက်ကျန် ၅၀ ရှိတယ် – လို့ အဖြေရပါတယ်။

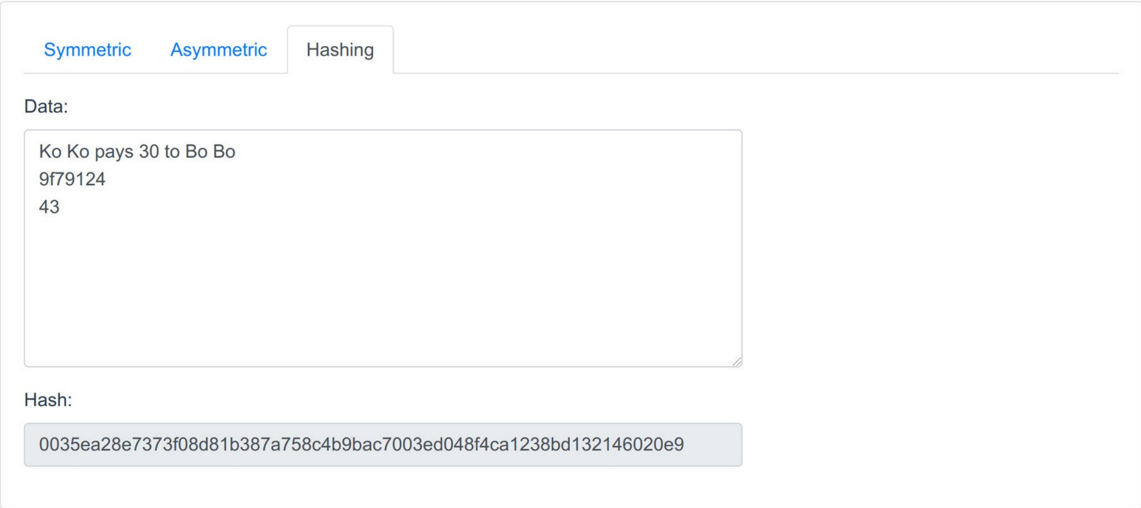
ဒီတော့မှ ကိုကိုက ဘိုဘိုကို ၃၀ ပေးတယ်ဆိုတဲ့ အပေးအယူမှတ်တမ်းပါတဲ့ Block ကိုထည့်လို့ရမှာပါ။ အခုနမူနာမှာ Block သုံးလေးခုပဲရှိလို့ တွက်ရတာ ဘာမှမခက်ပါဘူး။ လက်တွေ့မှာ အသုံးပြုသူများပြီး အချိန်ကြာလာတာနဲ့အမျှ Blockchain တစ်ခုမှာ Block ပေါင်း တစ်ရာတစ်ထောင်ကနေ၊ တစ်သန်း၊ သန်း တစ်ထောင် ဆိုတာမျိုးထိ ဖြစ်လာမှာပါ။ အဲ့ဒီလောက် ပမာဏကနေ တွက်ယူနိုင်ဖို့ဆိုတာတော့ မလွယ် တော့ပါဘူး။ တွက်ယူနိုင်စွမ်းရှိသူ ဖြစ်ဖို့လိုလာပါတယ်။ အခု နဲသေးပေမယ့် အခုကတည်းက အဲ့ဒီလို တွက် ယူနိုင်စွမ်း ရှိသူဆိုတာကို သက်သေပြဖို့ လိုပါတယ်။ အဲ့ဒီလို တွက်ယူနိုင်စွမ်းရှိတဲ့သူကိုမှသာ Block အသစ် ထည့်ခွင့်ပေးမှာ ဖြစ်ပါတယ်။

ဒါကြောင့် Proof of Work ခေါ် တွက်ယူနိုင်စွမ်းရှိသူ ဖြစ်ကြောင်း သက်သေပြခြင်း လုပ်ငန်းစဉ် လိုအပ်လာ ပါတယ်။

Block တစ်ခုကို Hash လုပ်လိုက်တဲ့အခါ ရလာမယ့် Hash တန်ဖိုးဘာဖြစ်မလဲဆိုတာ ကြိုမသိနိုင်ပါဘူး။ အဲ့ဒီ Hash တန်ဖိုးမှာ ရှေ့ဆုံးကနေ 00 ဆိုတဲ့ သုညနှစ်လုံးနဲ့ စရမယ်။ 00 နှစ်လုံးမစရင် စသွားအောင် တန်ဖိုးတစ်ခုကို တွဲပေးရမယ်လို့ သတ်မှတ်လိုက်ပါမယ်။

ဥပမာ – ထည့်ချင်တဲ့ Data က Ko Ko pays 30 to Bo Bo ဆိုရင် အဲ့ဒီ Data ကို Previous Hash ဖြစ်တဲ့ 9f79124 နဲ့ တွဲပြီး Hash လုပ်ရပါတယ်။ ရလဒ်က **2933d1b** ဖြစ်ပါတယ်။ ရှေ့ဆုံးက 00 နဲ့မစပါဘူး။ ဒါ ကြောင့် 1 ဆိုတဲ့ တန်ဖိုးတစ်ခု ထပ်ထည့်ပြီး Hash လုပ်လိုက်တဲ့အခါ **cf30549** ကို ရပါတယ်။ ရှေ့ဆုံးက 00 နဲ့ မစသေးပါဘူး။ ဒါကြောင့် 2 ဆိုတဲ့တန်ဖိုးတစ်ခု ထပ်ထည့်ပြီး Hash လုပ်ကြည့်တဲ့အခါ **2b41ea8** ကိုရပါ တယ်။ လိုချင်တဲ့ရလဒ် မဟုတ်သေးပါဘူး။ ဒီလိုနဲ့ တန်ဖိုးတစ်ခုပြီးတစ်ခု ထပ်တိုးတိုးကြည့်လိုက်တဲ့အခါ နောက်ဆုံးမှာ **43** ဆိုတဲ့တန်ဖိုးထည့်ပြီး Hash လုပ်ကြည့်လိုက်တဲ့အခါ **0035ea2** ဆိုတဲ့ ရလဒ်ကို ရပါတော့ တယ်။ 00 နဲ့ စသွားပြီမို့လို့ လိုချင်တဲ့ရလဒ် ရသွားပါပြီ။

ဒီရလဒ်ရဖို့အတွက် 43 ကြိမ် အလုပ်လုပ်ခဲ့ရပါတယ်။ နမူနာမှာ Hash တွေကို အတိုကောက်ရေးခဲ့ပေမယ့် ရှေ့ဆုံး (၇) လုံး ဖြတ်ယူထားတဲ့ တစ်ကယ့် Hash အစစ်တွေပါ။ ဒါကြောင့် လက်တွေ့စမ်းကြည့်နိုင်ပါတယ်။ စမ်းကြည့်ဖို့ တိုက်တွန်းပါတယ်။



နမူနာကို ဂရုပြုကြည့်ပါ။ ရလာတဲ့ Hash တန်ဖိုးက ရှေ့ဆုံးမှာ 00 နဲ့စနေပါတယ်။ အဲ့ဒီလို 00 နဲ့စတဲ့ရလဒ် ရဖို့အတွက် 1, 2, 3, 4 တစ်ခုပြီး တစ်ခု Data ထဲကို ပေါင်းထည့်ကြည့်ပြီး 43 ကြိမ်မြောက်မှာ လိုချင်တဲ့ ရလဒ်ကို ရသွားတာပါ။ လိုချင်တဲ့အဖြေ ရသွားပြီဆိုတဲ့သဘောပါပဲ။

ဒီလိုမျိုးလိုချင်တဲ့ Hash ရလဒ်ရအောင် တွက်ယူတဲ့ လုပ်ငန်းစဉ်ကို Proof of Work လို့ခေါ်တာပါ။ ရလာတဲ့ ရလဒ်နဲ့အတူ Blockchain ထဲမှာ Block အသစ်ကို ထည့်ခွင့်ပြုမှာပဲ ဖြစ်ပါတယ်။ ဒါကြောင့် လက်ရှိနမူနာ Blockchain ရဲ့ပုံစံက အခုလို ဖြစ်ပါလိမ့်မယ်။

...	Block #2 →	Block #3 →	Block #4 →
...	Data Ko Ko pays 50 to Ni Ni	Data Bo Bo buys a game for 120	Data Ko Ko pays 30 to Bo Bo
...	Previous Hash d789979	Previous Hash 2b72935	Previous Hash 9f79124
...	Hash 2b72935	Hash 9f79124	Hash 0035ea2
...			Nonce 43

ရရှိခဲ့တဲ့အဖြေ 43 ကို **Nonce** အနေနဲ့ တွဲသိမ်းထားပါတယ်။ Nonce ဆိုတာ Number Only Used Once ရဲ့ အတိုကောက်ပါ။ လိုချင်တဲ့ Hash ရလဒ် ရဖို့အတွက် ထည့်ပေါင်းရတဲ့ နံပါတ်ကို Nonce လို့ ခေါ်ကြတာပါ။

ဒါက မြင်ရလွယ်အောင်ပေးတဲ့နမူနာမို့လို့ပါ။ တစ်ကယ့် Bitcoin ရဲ့ Proof of Work က Hash ရဲ့ ရှေ့ကနေ သုည ဆယ်လုံးကျော်ထိ ပါအောင် တွက်ခိုင်းတာပါ။ ဆယ်လုံးကျော်လေးပဲဆိုပြီး အထင်မသေးပါနဲ့။ တစ်လုံးတိုးတိုင်း ဆတိုးနဲ့ခက်သွားတာပါ။ အကြိမ်ပေါင်း ထရီလီယံနဲ့ချီပြီး တွက်ချက်နိုင်မှသာ လိုချင်တဲ့ ရလဒ်ကို ရမှာပါ။ အတိအကျ မပြောဘဲ ဆယ်လုံးကျော်လို့ ပြောတာကတော့ တွက်တဲ့သူ များရင်များသလို တွက်ရ ခက်သထက်ခက်အောင် လုပ်တဲ့သဘောရှိလို့ပါ။ တွက်တဲ့သူများလို့ပဲ ဖြစ်ဖြစ်၊ တွက်နိုင်တဲ့ စွမ်းအား ကောင်းလို့ပဲ ဖြစ်ဖြစ်၊ အဖြေ ခဏလေးနဲ့ ထွက်နေရင် ပိုခက်သွားအောင် ရှာရတဲ့ သုည အရေအတွက်ကို တိုးပြီး ရှာခိုင်းပါတယ်။ ဒါကြောင့် တွက်ချက်မှုပေါင်း ထရီလီယံနဲ့ချီပြီး အချိန် (၁၀) မိနစ် ခန့်ကြာအောင် တွက်ယူမှသာ အဖြေမှန်ကို ရလေ့ရှိတာပါ။

နမူနာအနေနဲ့ ဒီ Bitcoin Block ကို လေ့လာကြည့်ပါ။

https://www.blockchain.com/btc/block/675817

Blockchain.com Wallet Exchange Explorer

Hash	00000000000000000002d6ec7a06bb3803674ee3acdb9458b9360e4d15bf0037
Confirmations	12,456
Timestamp	2021-03-23 01:16
Height	675817
Miner	BTC.TOP
Number of Transactions	3,091
Difficulty	21,865,558,044,610.55
Merkle root	0135360c9f1fc7f07a954656781042f3af9d87fef41ca7bbaacf6b1da9b03175
Version	0x20000000
Bits	386,719,599
Weight	3,992,924 WU
Size	1,279,277 bytes
Nonce	625,538,777

Bitcoin Block 675817

၂၀၂၁ ခုနှစ်၊ မတ်လ (၂၃) ရက်နေ့မှာ တွက်ချက်အောင်မြင်ခဲ့ပြီး ရှေ့ကနေ သုည (၁၉) လုံးနဲ့ စတဲ့ Hash ကိုရအောင် တွက်ချက်ခဲ့ရတဲ့ Block ပါ။ အဖြေမှန် **Nonce** တန်ဖိုးကတော့ **625,538,777** ဖြစ်ပါတယ်။ ဒီလို တွက်ပေးတဲ့အတွက် ဆုအနေနဲ့ **6.25 BTC** ကို ရရှိသွားပါတယ်။ ဒီစာရေးနေတဲ့အချိန် Bitcoin ရဲ့ ပေါက်ဈေးက 1 BTC = 34,015 USD ဖြစ်တဲ့အတွက် ဒေါ်လာ (၂) သိန်းကျော် တန်ဖိုးရှိတဲ့ ဆုကိုရရှိသွားတာပါ။

တစ်လက်စထဲ ထည့်မှတ်ထားရမှာကတော့ ငွေကြေးအရောင်းအဝယ်ဈေးကွက်မှာ အမေရိကန် ဒေါ်လာ အတွက် Currency Code အနေနဲ့ USD ကို အသုံးပြုပြီး၊ စင်ကာပူဒေါ်လာဆိုရင် SGD၊ မြန်မာကျပ်ဆိုရင် MMK စသည်ဖြင့် သတ်မှတ်အသုံးပြုကြသလိုပဲ Bitcoin ရဲ့ Currency Code အနေနဲ့ **BTC** ကို သတ်မှတ် အသုံးပြုကြပါတယ်။

Bitcoin အကြောင်းကို လေ့လာသူအများစု သိချင်ကြတဲ့ Bitcoin Mining ဆိုတာ ဒါကိုပြောနေတာပါ။ လိုအပ်တဲ့တွက်ချက်မှုကို လုပ်ပြပြီး Block တွေထည့်သွင်းပေးခြင်းအားဖြင့် ဆုငွေထုတ်ယူတဲ့ လုပ်ငန်းဖြစ်ပါတယ်။ ဒီအကြောင်းကို နောက်တစ်ခန်းမှာ သပ်သပ် ထပ်ပြောပါဦးမယ်။

Distributed Ledger

Blockchain ထဲမှာ သိမ်းဆည်းထားတဲ့ အချက်အလက်တွေကို တစ်စုံတစ်ဦး၊ အဖွဲ့အစည်းတစ်ခုက တာဝန်ခံ သိမ်းဆည်းထားတာမျိုး မဟုတ်ပါဘူး။ ကွန်ပျူတာ Network ကွန်ယက်ထဲမှာ ခွဲဖြန့် ကူးယူ သိမ်းဆည်းထားကြတာပါ။ သင့်တော်တဲ့ ဆော့ဖ်ဝဲရှိတဲ့ ဘယ်ကွန်ပျူတာမဆို Bitcoin Network မှာ Node တစ်ခုအနေနဲ့ ပါဝင်လို့ရပါတယ်။ ပြန်ထွက်ချင်တဲ့အချိန် အချိန်မရွေး ပြန်ထွက်လို့ရပါတယ်။

သင့်တော်တဲ့ဆော့ဖ်ဝဲဆိုတာ Bitcoin Core လို ဆော့ဖ်ဝဲမျိုးကို ပြောတာပါ။ Bitcoin Core မှ မဟုတ်ပါဘူး။ Bitcoin Network ကို ချိတ်ဆက်ပြီး Blockchain ဒေတာတွေကို Download ရယူပေးနိုင်တဲ့ ဘယ်ဆော့ဖ်ဝဲမဆို ချိတ်ဆက်ပါဝင်လို့ရပါတယ်။

Bitcoin Core – https://bitcoin.org/en/bitcoin-core/

ကိုယ့်ကွန်ပျူတာက Bitcoin Network မှာ Node တစ်ခုအနေနဲ့ ပါဝင်သွားပြီဆိုရင် ကိုယ့်ဆီမှာ Blockchain မိတ္တူတစ်စုံ ရရှိသွားတာပါပဲ။ မူအရ ကိုယ်တိုင်လည်း အထက်မှာ ပြောခဲ့သလို Proof of Work ကို ပြပြီး Block တွေထည့်နိုင်ရင် ထည့်ပေးလို့ ရပါတယ်။ မူအရလို့ စကားခံထားတာက တစ်ကယ်ထည့်ဖို့ကတော့ လွယ်တဲ့အလုပ် မဟုတ်လို့ပါ။ ထည့်လို့ရတယ်၊ ထည့်ပေးလိုက်တယ်လို့ပဲ သဘောထားပါ။ ကိုယ်ထည့်ပေးလိုက်တဲ့ Block အသစ်ကို Broadcast လုပ်ပြီး Network ထဲမှာပါဝင်တဲ့ တစ်ခြား Node တွေဆီကို ဖြန့်ဖြူးပေးလိုက်မှာပါ။ တစ်ခြား Node တွေကနေ ထည့်ပေးလိုက်တဲ့ Block အသစ်တွေကလည်း သူတို့ဆီကနေ Broadcast လုပ်ပြီး ပို့ပေးလိုက်လို့ ကိုယ့်ဆီက မိတ္တူမှာလည်း Update ဖြစ်ပြီး ထပ်တိုးသွားမှာ ဖြစ်ပါတယ်။

ထပ်တိုးလိုက်တဲ့ Block ဟာ တိကျမှန်ကန်မှု ရှိမရှိကိုလည်း Node တွေက ဝိုင်းဝန်းစိစစ် Validate လုပ်ကြဦးမှာပါ။ Validate လုပ်တယ်ဆိုတာ ထည့်လိုက်တဲ့ Block က နှစ်ယောက်ထည့်မိလို့ Duplicate ဖြစ်နေ

သလား၊ Hash တွေ Nonce တွေ မှန်ရဲ့လား၊ အထဲမှာပါတဲ့ Transaction တွေမှန်ရဲ့လား၊ စသည်ဖြင့် စစ်တာပါ။ မှန်တယ်ဆိုရင် Confirm လုပ် ထည့်သွင်းပေးလိုက်မှာ ဖြစ်ပြီးတော့ မမှန်ရင်တော့ Reject လုပ်လိုက်မှာပါ။ Confirm လုပ်ထားတဲ့အရေအတွက် တချို့ရရင်တော့ ကျန် Node တွေက ထပ်ပြီး Confirm လုပ်နေစရာ မလိုတော့ပါဘူး။ စိတ်ချလက်ချ Update လုပ်လိုက်ယုံပါပဲ။

ကိုယ့်ဆီမှာရှိနေတဲ့ မိတ္တူနဲ့ သူများဆီမှာရှိနေတဲ့ မိတ္တူ တစ်စုံတစ်ရာ ကွဲလွဲမှု ရှိခဲ့ရင် ပိုပြီးတော့ Update ဖြစ်တဲ့ မိတ္တူကို အတည်ယူပြီးတော့ ညှိပေးသွားမှာပါ။ ဒီနည်းနဲ့ တူညီပြီး Update ဖြစ်တဲ့ မိတ္တူတွေ Network ထဲမှာ အနှံ့အပြားရှိနေလို့ တစ်စုံတစ်ဦးက မသမာတဲ့ နည်းနဲ့ ပြင်ဆင်ဖို့ဆိုတာ ဘယ်လိုမှမလွယ်တော့ပါဘူး။

ဒါကြောင့် အထက်မှာ မေးခွန်းထုတ်ခဲ့တဲ့ ကြားဖြတ်မပြင်ဘဲ နောက်ဆုံး Block တစ်ခုနှစ်ခုပဲ ပြင်လို့လည်း မရနိုင်ပါဘူး။ Distributed Ledger ဖြစ်နေလို့ပါ။ Invalid Block အနေနဲ့ တစ်ခြား Node တွေက Reject လုပ်လိုက်မှာဖြစ်ပြီး ပိုပြီး Update ဖြစ်တဲ့ Blockchain အမှန်နဲ့ အစားထိုးသွားမှာ မို့လို့ပါ။ ကြားဖြတ်ပြင်ပြီး နောက်ဆက်တွဲ ရှိသမျှ အကုန်ပြင်မယ်ဆိုတာကတော့ ပိုဆိုးသွားပါပြီ။ အတွဲလိုက် ပြင်ရမယ့် Block တိုင်းအတွက် Proof of Work ကို ပြရတော့မှာဖြစ်လို့ ပိုပြီးတော့ မဖြစ်နိုင်တော့ပါဘူး။

51% Attack

ဒီလို Blockchain ထဲက Data ကို တိုက်ရိုက် ပြင်လို့မရပေမယ့် အနှောက်အယှက်ပေးလို့ရတဲ့ နည်းတော့ ရှိပါသေးတယ်။ 51% Attack လို့ခေါ်ပါတယ်။ <u>လူတစ်ဦးရဲ့ Node က</u> (သို့) အဖွဲ့အစည်းတစ်ခုရဲ့ Node များက <u>Network ထဲမှာပါဝင်တဲ့ တစ်ခြား Node ၅၀% ထက်ပိုပြီး တွက်ချက်နိုင်စွမ်း စွမ်းဆောင်ရည် မြင့်နေတဲ့ အခြေအနေမှာ</u> Network ကို သူက ချယ်လှယ်လို့ ရသွားပါတယ်။

ကိုကို၊ ဘိုဘို နဲ့ နီနီ တို့ (၃) ဦးမှာ ဘိုဘိုက အရမ်းတော်လို့ သူကချည်းပဲ သူများထက် အဖြေမှန် အရင်ရအောင် အမြဲရှာနိုင်နေရင် သူကချည်းပဲ ထပ်တိုး Block တွေကို ထည့်သွားတဲ့အခါ သူထည့်ချင်ရာ ထည့်လို့ရကောင်း ရသွားမှာပါ။ ဒါကြောင့် ကိုကို နဲ့ နီနီက တစ်ယောက်ချင်းမတွက်တော့ဘဲ နှစ်ယောက်ပေါင်းတွက်လိုက်လို့ ဘိုဘိုထက် သာအောင်တွက်နိုင်ရင် 51% Attack မဖြစ်တော့ပါဘူး။ ဘိုဘိုက တော်လွန်းအားကြီးလို့ နှစ်ယောက်ပေါင်းတွက်တာတောင် မနိုင်တော့ဘူးဆိုရင်တော့ 51% Attack ဖြစ်နိုင်သွားပါပြီ။

ဒီလိုပါပဲ။ Bitcoin Network မှာ ကွန်ပျူတာ (၁၀) လုံးနဲ့ စုစုပေါင်း Node (၁၀) ခု ပါဝင်ပေမယ့် လူတစ်ယောက်ထဲက ကွန်ပျူတာ (၆) လုံးသုံးပြီး Node (၆) ခုစာ ပါဝင်ချိတ်ဆက်ထားပြီး၊ Proof of Work ကို ပြဖို့အတွက် အဲ့ဒီ (၆) လုံးပေါင်း စွမ်းအားနဲ့ တွက်တဲ့အခါ သူကချည်းပဲ အမြဲအဖြေရနေလို့ ကျန်တဲ့ Node တွေက ထည့်ခွင့်မရတော့တာမျိုး ဖြစ်သွားတော့မှာပါ။ ကျန် Node (၄) ခုက အတူတူပေါင်းပြီး အလုပ်လုပ်ရင်တောင် သူ့ကို မမှီနိုင်တော့ပါဘူး။

ဒီအခါမှာ Block အသစ်တွေ ထည့်တဲ့အခါ၊ အထဲမှာ ဘယ် Transaction တွေကိုထည့်မယ်၊ ဘယ် Transaction တွေကိုမထည့်ဘူးဆိုတာ သူကြိုက်သလို ချယ်လှယ်လို့ ရသွားပါပြီ။ ဒီသဘောကို 51% Attack လို့ ခေါ်တာပါ။

ဒီပြဿနာက အထူးသဖြင့် Network မှာပါဝင်တဲ့ Node တွေ နည်းစဉ်မှာ ကြုံရတာပါ။ ပါဝင်တဲ့ Node များရင်တော့ ဖြစ်နိုင်ခြေနည်းသွားပါတယ်။ ဥပမာ – Node အခု (၁၀,၀၀၀) ရှိတယ်ဆိုရင် 51% Attack လုပ်ချင်တဲ့သူက Node (၅,၀၀၀) ကျော်ထက်ပိုသာတဲ့ စွမ်းဆောင်ရည်ကို ရမှဖြစ်ပါတော့မယ်။ ဒီစွမ်းဆောင်ရည်ကိုရဖို့ အသုံးပြုရမယ့် ရင်းနှီးမြှုပ်နှံမှုက ပြန်ရမယ့်ရလဒ်နဲ့ မကာမိနိုင်တော့ပါဘူး။

Coinbase

Proof of Work ကို ပြပြီး Block အသစ်တွေကို ထည့်ပေးလိုက်ရင် ဆုငွေရပါတယ်။ အဲ့ဒီဆုငွေ ဘယ်ကရတာလဲဆိုတာ မေးစရာ ရှိလာပါတယ်။ ဒီနေရာမှာ Coinbase လို့ခေါ်တဲ့ သဘောသဘာဝ ဝင်လာပါတယ်။

မှတ်ချက် ။ ။ Coinbase.com လို့ခေါ်တဲ့ Cryptocurrency Exchange တစ်ခုလည်း ရှိနေပါတယ်။ အခု ဖော်ပြမယ့် Coinbase ဟာ အဲ့ဒီ Coinbase.com Exchange ကို ဆိုလိုခြင်း မဟုတ်ပါဘူး။

Coinbase ဟာ ဘာနဲ့တူလည်းဆိုတော့ ရွှေတွေ ကြိုထည့်ပြီး အသေပိတ်ထားတဲ့ Safe Box နဲ့ တူပါတယ်။ အထဲကငွေကို ထုတ်ယူချင်ရင် တစ်ခြားနည်းလမ်း မရှိပါဘူး၊ Proof of Work ကို ပြပြီး ခလုပ်နှိပ်မှသာ သတ်မှတ်ဆုငွေ ပမာဏကို ထုတ်ပေးမှာပါ။ <u>Proof of Work ကိုပြတယ်ဆိုတာ Coinbase ထဲမှာရှိနေတဲ့ ရွှေတွေ ထွက်လာအောင် တူးယူတဲ့ သဘောမို့လို့ Mine လုပ်တယ်လို့ ဆိုကြတာပါ</u>။

ဒါကြောင့် ခဏခဏမေးခံရတဲ့ ဒီမေးခွန်းကို ထပ်ပြောချင်ပါတယ်။ Bitcoin မှာ Mine လုပ်တယ်ဆိုတာ ပေါက်တူး ဂေါ်ပြားတွေနဲ့ ကျောက်တောင်ထဲက ရွှေကို တူးယူသလို အမှန်တစ်ကယ် တူးယူတာမျိုး မဟုတ်ပါဘူး။ Coinbase ထဲက ရွှေတွေ ထွက်လာအောင် Proof of Work ကို ပြတာပါ။ ကျောက်တောင်ကို တူးဖို့ ပေါက်တူး ဂေါ်ပြားတွေ လိုသလိုပဲ Coinbase ထဲက ရွှေထွက်လာအောင် Proof of Work ကိုပြဖို့ လိုအပ်တဲ့တွက်ချက်မှုတွေ လုပ်နိုင်တဲ့ ကွန်ပျူတာစက်တွေ လိုအပ်တာပါ။

အထက်မှာ နမူနာပေးခဲ့တဲ့ Blockchain ကို Coinbase ဆိုတဲ့ သဘောသဘာဝ ပါသွားအောင် အခုလို ပြင်လိုက်ချင်ပါတယ်။

Genesis Block →	**...**	**Block #3 →**	**Block #4 →**
Coinbase **300**	...	Coinbase **300**	Coinbase **310**
Data Dad pays Ko Ko, Bo Bo & Ni Ni 100 each	...	Data Bo Bo buys a game for 120	Data Ko Ko pays 30 to Bo Bo
Previous Hash 0000000	...	Previous Hash 2b72935	Previous Hash 9f79124
Hash 95cc830	...	Hash 9f79124	Hash 0035ea2
			Nonce **43**
			Reward **10**

စစခြင်း Genesis Block မှာ Coinbase ကနေ **300** ထုတ်ယူထားပါတယ်။ Proof of Work ကို ပြစရာမလိုဘဲ ခြွင်းချက်အနေနဲ့ ထုတ်ယူလိုက်တဲ့ ပမာဏပါ။

Bitcoin ကတော့ ဒီလိုခြွင်းချက်နဲ့တောင် ကြိုမထုတ်ပါဘူး။ နောက်မှပဲ Proof of Work ကိုပြပြီး ထုတ်ယူတာပါ။ အခုပေးထားတဲ့ နမူနာမှာတော့ အစပိုင်းမှာ Proof of Work မပါသေးလို့ ဒီတိုင်းပဲ 300 ကို Coinbase ကနေ ခြွင်းချက်နဲ့ ထုတ်ယူ ပြလိုက်တာပါ။ နောက်ပိုင်းတော့ မရတော့ပါဘူး။ Proof of Work

ကို ပြမှပဲ ထုတ်ပေးတော့မှာပါ။ ဒါကြောင့် နောက်ဆုံး Proof of Work ကို ပြနိုင်တဲ့ Block #4 ကျတော့မှ ဆုငွေအဖြစ် ထုတ်ပေးလိုက်တဲ့ 10 ကို Coinbase ကနေ ထုတ်ပေးလိုက်တာပါ။ ဒါကြောင့် နမူနာအရ Coinbase ကနေ ထုတ်ပေးပြီး စုစုပေါင်း ပမာဏ **310** ဖြစ်သွားပြီပဲ ဖြစ်ပါတယ်။

တချို့ Cryptocurrency တွေမှာ Coinbase ကနေ ဘယ်လောက်ထိ ထုတ်ပေးမှာလဲဆိုတဲ့ အကန့်အသတ် မရှိပါဘူး။ Proof of Work ကိုပြပြီး Block အသစ်ထည့်နေသ၍ ထုတ်ပေးနေမှာပါပဲ။ တစ်ကယ်တော့ ငွေစက္ကူပမာဏ ဘယ်လောက်ဖြစ်သွားရင် ရိုက်မထုတ်ရတော့ဘူးလို့ ကန့်သတ်ထားတာမျိုး ရှိလေ့မရှိလို့ Fiat Currency ဆိုတာလည်း မူအရ အကန့်အသတ်မရှိ ထုတ်လို့ရတဲ့ ငွေကြေး တစ်မျိုးပဲဆိုတာကို ထည့်သွင်းမှတ်သားသင့်ပါတယ်။

တချို့ Cryptocurrency တွေကတော့ Coinbase ကနေ ဘယ်လောက်ထိပဲ အမြင့်ဆုံး ထုတ်ပေးရမယ်ဆိုတဲ့ ကန့်သတ်ချက်ရှိပါတယ်။ သတ်မှတ်ပမာဏကို ရောက်ရင် ထပ်ထုတ်ပေးခွင့်မရှိတော့ပါဘူး။ ဒီလို ထပ်ထုတ်ပေးလို့ မရတော့အောင် မူလစနစ်ဒီဇိုင်းမှာ တစ်ခါထဲ ထည့်သွင်းတည်ဆောက် ထားကြသလို Network မှာ ပါဝင်ကြတဲ့ Node တွေကလည်း လက်ခံကြမှာ မဟုတ်လို့ ထုတ်လို့ရတဲ့နည်းလမ်း ရှိမှာ မဟုတ်ပါတယ်။ Bitcoin က အဲ့ဒီလိုမျိုး ကန့်သတ်ထားတဲ့ Cryptocurrency ဖြစ်ပါတယ်။ ဒါကြောင့် သတ်မှတ် ကွိုင်အရေအတွက် ပြည့်သွားရင် ထပ်ထွက်လာတော့မှာ မဟုတ်ပါဘူး။

ဘယ်လောက်မှာ ကန့်သတ်ထားတာလဲ ဆိုတာကိုတော့ အချက်အလက်တွေကို ပြန်ကျဲနေမှာစိုးလို့ ခဏနေမှ တစ်စုတစ်စည်းထဲ ဖော်ပြပါမယ်။ ဒီနေရာမှာတော့ Coinbase ကနေ ထွက်တဲ့ ပမာဏ အကန့်အသတ်ရှိတဲ့ Cryptocurrency ရှိသလို၊ အကန့်အသတ်မရှိတဲ့ Cryptocurrency လည်းရှိတယ် ဆိုတာကို မှတ်သားထားရမှာပဲ ဖြစ်ပါတယ်။ ငွေပေးငွေယူ မှတ်တမ်းစာရင်းကို ရှင်းလိုက်ရင် နောက်ဆုံးရလဒ်ဟာ Coinbase ကနေ ထုတ်ပေးထားတဲ့ ပမာဏနဲ့ လုံးဝကွက်တိပဲ အမြဲတမ်း ဖြစ်နေရမှာပါ။

စာရေးသူအနေနဲ့ Bitcoin ပေါ်ခါစက သူ့အကြောင်းကိုလေ့လာကြည့်တဲ့အခါ လက်ခံဖို့အခက်ဆုံး ဖြစ်ခဲ့တာကတော့ ဒီ Coinbase ဆိုတဲ့သဘောတရားပါပဲ။ Proof of Work ကို ပြမှ ထွက်လာတယ် ဆိုပေမယ့် တစ်ကယ်တမ်း အရင်းစစ်တော့ သူ့အလိုလို လေထဲက ထွက်လာတဲ့ ငွေတွေပါပဲ။ တစ်နေရာရာကနေ၊ တစ်ခြားတန်ဖိုးရှိတဲ့အရာ တစ်ခုခုကနေ ပြောင်းလဲဖြစ်ပေါ်လာခြင်း မဟုတ်ပါဘူး။ ဒီလို လေထဲကထွက်လာတဲ့ ငွေမှာ တန်ဖိုးရှိတယ်ဆိုတာ လက်ခံဖို့ခက်ခဲနေတာပါ။

တစ်ကယ်တော့ Fiat Money ဆိုတာလည်း ဒီလိုပဲ မူလတန်ဖိုးရှိတဲ့အရာကနေ ပုံစံပြောင်းလဲ ဖြစ်ပေါ်လာတာ မဟုတ်ဘဲ လိုအပ်တဲ့အချိန် ရိုက်ထုတ်လိုက်တဲ့ အရာတွေပါပဲ။ ဒါပေမယ့် ဗဟိုဘဏ်လို အာဏာပိုင်အဖွဲ့အစည်းတွေက တန်ဖိုးရှိတယ်လို့ အာမခံပေးပြီး အများက အဲ့ဒီအာမခံချက်ကို ယုံကြည်လို့သာ တန်ဖိုးရှိကြတာပါ။ ဒီငွေဟာ ရွှေလို အဖိုးတန်သတ္တု မဟုတ်ပေမယ့် များလက်ခံကြတဲ့ ကြားခံဖလှယ်အသုံးပြုနိုင်ခြင်းဆိုတဲ့ ဂုဏ်သတ္တိလည်း ရှိနေပါတယ်။

ဒီလိုစဉ်းစားကြည့်လိုက်တဲ့အခါ Bitcoin ဟာလည်း ဂုဏ်သတ္တိမဲ့အရာတစ်ခု မဟုတ်တော့ပါဘူး။ <u>လုံခြုံစိတ်ချစွာ သိမ်းဆည်းထားနိုင်ခြင်းနဲ့ ကိုယ်တိုင်တိုက်ရိုက်ဖလှယ်နိုင်ခြင်းဆိုတဲ့ ဂုဏ်သတ္တိတွေရှိနေပါတယ်။</u> "ကိုယ်တိုင်" ဆိုတာလေးက အရေးကြီးပါတယ်။ ဒီလိုအချက်တွေကြောင့်ပဲ အသုံးပြုကြသူ အများက တန်ဖိုးရှိတယ်လို့ လက်ခံလိုက်ကြတဲ့အခါမှာ တန်ဖိုးရှိတဲ့အရာတစ်ခု ဖြစ်သွားတော့တာပါပဲ။

နည်းပညာပိုင်းက လက်ခံရ မခက်လှပေမယ့်။ ဒီသဘောသဘာဝကတော့ လက်ခံရခက်ခဲတဲ့ သဘောဖြစ်နိုင်ပါတယ်။ လက်တွေ့ဈေးကွက်မှာလည်း Bitcoin ကို တစ်ကယ့်အဖိုးတန် အရာတစ်ခုအနေနဲ့ လက်ရှိဖလှယ် ရောင်းဝယ်နေကြသူတွေ အများကြီးရှိသလို၊ Bill Gates တို့ Warren Buffet တို့လို လူတွေအပါအဝင် Bitcoin ရဲ့ သဘောကို လက်မခံနိုင်ကြသူတွေလည်း အများကြီးပါ။ စာဖတ်သူအနေနဲ့ ဒီသဘောတရားကို လက်ခံနိုင်ခြင်း ရှိမရှိဆိုတာကတော့ စာဖတ်သူကိုယ်တိုင်ပဲ သုံးသပ်ဆင်ခြင်ရမှာပါ။ စာရေးသူကတော့ လက်ခံဖို့ လက်မခံဖို့ တိုက်တွန်းနေခြင်းမဟုတ်ဘဲ၊ ရှိနေတဲ့ သဘောကို တင်ပြခြင်းသာဖြစ်ပါတယ်။

Account (Address)

ငွေပေးငွေယူမှတ်တမ်းတွေ သိမ်းတဲ့အခါ ပေးခဲ့တဲ့ Blockchain နမူနာအရ အထဲမှာ လူနာမည်တွေ ပါဝင်နေပါတယ်။ တစ်ကယ့်လက်တွေ့မှာ အဲ့ဒီမှတ်တမ်းတွေ ပါဝင်တဲ့ Distributed Ledger ဆိုတာ ဘယ်သူမဆို ကြည့်ရှုနိုင်တဲ့ အရာတွေပါ။ ဒီလို လူတိုင်းကြည့်လို့ရတဲ့ စာရင်းထဲမှာ ကိုယ့်ရဲ့ငွေပေးငွေယူ ကိစ္စလို အရေးကြီးတဲ့ တစ်ကိုယ်ရေ အချက်အလက်ကို လူနာမည်ကြီးနဲ့ တွဲပါနေလို့တော့ မဖြစ်ပါဘူး။ ပြီးတော့ လူနာမည် သက်သက်နဲ့လည်း ပေးချေမှုကို အတည်ပြုလို့ မရနိုင်ပါဘူး။ ဘိုဘိုက နီနီ ကို ငွေ ၂၀ ပေးပါတယ် လို့ မှတ်တမ်းတင်ထားပေမယ့် ဘိုဘိုက တစ်ကယ်ပေးချေကြောင်း၊ နီနီက အမှန်တစ်ကယ် လက်ခံရရှိကြောင်း အတည်ပြုနိုင်ဖို့ လိုပါသေးတယ်။

ဒီနေရာမှာ အသုံးဝင် လာတာကတော့ ရှေ့ပိုင်းမှာ လေ့လာခဲ့တဲ့ Public Key Encryption နဲ့ Digital Signature တို့ ပါပဲ။

ငွေပေးငွေယူလုပ်ငန်းတွေ ဆောင်ရွက်ဖို့အတွက် ဘဏ်တွေမှာ အကောင့်ဖွင့်ရသလိုပဲ Cryptocurrency မှာလည်း အကောင့် လိုပါတယ်။ ဒါပေမယ့် အဲ့ဒီအကောင့်ဖွင့်ကို ဘယ်သူ့ဆီကမှ ခွင့်တောင်းစရာမလိုဘဲ ကိုယ်တိုင် ဖွင့်နိုင်ပါတယ်။ Public Key နဲ့ Private Key တစ်စုံ ထုတ်လိုက်ပြီး Public Key ကို အကောင့်အနေနဲ့ အသုံးပြုနိုင် ပါတယ်။ အကောင့်လို့တော့ မခေါ်ကြပါဘူး။ Address လို့ ခေါ်ကြပါတယ်။ ဒါကြောင့် Address လို့ဆက်သုံးသွားမှာ ဖြစ်ပေမယ့် ဒါဟာ ငွေပေးငွေယူ ပြုလုပ်နိုင်တဲ့ ဘဏ်အကောင့် သဘောသဘာဝ ဆင်တူတယ်လို့ မှတ်နိုင်ပါတယ်။ ဒီလိုမျိုး Public Key ကို Address အနေနဲ့ အသုံးပြုကြတဲ့အတွက် နမူနာပြခဲ့တဲ့ Blockchain မှာပါဝင်တဲ့ Transaction တွေက အခုလိုပုံစံ ဖြစ်သွားပါလိမ့်မယ်။

Genesis Block →	**...**	**Block #3 →**	**Block #4 →**
Coinbase 300	...	Coinbase 300	Coinbase 310
Data **Uinh3kd** pays **2UkmwDa, 2RmNkSj** & **SXLQZzr** 100 each	...	Data **2RmNkSj** buys a game for 120 from **2ffHhft**	Data **2UkmwDa** pays 30 to **2RmNkSj**
Previous Hash 0000000	...	Previous Hash 2b72935	Previous Hash 9f79124
Hash 95cc830	...	Hash 9f79124	Hash 0035ea2
			Nonce 43
			Reward 10

လူနာမည်တွေနဲ့ မဟုတ်တော့ပါဘူး။ သက်ဆိုင်ရာ Address တွေနဲ့ ဖြစ်သွားပါပြီ။ နမူနာအရ ကိုကို့ရဲ့ Address က **2UkmwDa** ဖြစ်ပါတယ်။ Transaction မှတ်တမ်းအရ ဒီ Address မှာ ငွေ ၁၀၀ ရှိနေပါတယ်။ ဒါကြောင့် ကိုကို့ မှာ ငွေ ၁၀၀ ရှိတယ်ဆိုတဲ့ သဘောပါပဲ။ ဒီ Address ကို ကိုကို ပိုင်ကြောင်း ဘယ်သူ့မှ သိစရာမလိုပါဘူး။

ဒါဆိုရင် ကိုကိုက ဒီ Address ထဲကငွေကို ဘယ်လို ပိုင်တာလဲ။ သုံးချင်ရင် ဘယ်လို သုံးရမှာလဲ။

ကိုကို့မှာ **2UkmwDa** ဆိုတဲ့ Public Key ရဲ့ အတွဲအဖက် Private Key ရှိရမှာပါ။ ဒီတော့မှ အဲ့ဒီ Address မှာ ရှိနေတဲ့ ငွေကို လိုအပ်လာတဲ့အချိန် Private Key နဲ့ လက်မှတ်ထိုး ထုတ်ယူခြင်း၊ လွှဲပို့ခြင်းကို ပြုလုပ်နိုင်မှာပါ။ မြင်သာအောင် ပြောရရင် Public Key က ဘဏ်အကောင့်ဖြစ်သွားပြီး Private Key က အဲ့ဒီ အကောင့်ထဲက ငွေကို ထုတ်လို့ရတဲ့ Password ဖြစ်သွားတာပါ။

ဒါက မြင်သာအောင် ပေးတဲ့ ဥပမာပါ။ တစ်ကယ့်လက်တွေ့မှာ Public Key ကို Address အနေနဲ့ တိုက်ရိုက် မသုံးပါဘူး။ Bitcoin Address တစ်ခုရဲ့ နမူနာပုံစံက အခုလိုပုံစံမျိုး ဖြစ်နိုင်ပါတယ်။

```
1PMycacnJaSqwwJqjawXBErnLsZ7RkXUAs
```

စာလုံးအကြီးအသေးနဲ့ ကိန်းဂဏန်း (၃၄) လုံးပါဝင်ပါတယ်။ ဒါဟာ Public Key ကို Hash လုပ်ပြီး ရလာတဲ့ရလဒ်ကို Base58 Encode လို့ခေါ်တဲ့နည်းနဲ့ ထပ်ဆင့် Encode လုပ်ထားတာပါ။ Address တိုင်းဟာ အမြဲတမ်း ဒီပုံစံဖြစ်မယ်လို့ ပုံသေမှတ်လို့တော့ မရပါဘူး။ တစ်ခြား Address ဖန်တီးယူတဲ့ နည်း မူကွဲတွေ ရှိသေးလည်း ပုံစံအနည်းငယ် ကွဲပြားနိုင်ပါတယ်။ ဒီလိုပုံစံလည်း ဖြစ်နိုင်ပါသေးတယ်။

```
bc1qar0srrr7xfkvy5l643lydnw9re59gtzzwf5mdq
```

Base58 Encode အကြောင်းကိုတော့ Cryptography အကြောင်း ပြောတုံးက ထည့်မပြောခဲ့ရပါဘူး။ တစ်ကယ်တမ်းပြောမယ်ဆိုရင် Base64 တို့ Binary တို့ပါ ထည့်ပြောရမှာမို့လို့ မလိုအပ်ဘဲ အရမ်းရှုပ်သွားမှာစိုးလို့ ချန်ခဲ့လိုက်တာပါ။ အခုတောင် တော်တော်ရှုပ်နေလောက်ပါပြီ။ Public Key က စာလုံး (၆၄) လုံးပါဝင်ပြီး ကိန်းဂဏန်းတွေများလို့ ရိုက်ထည့်ရခက်တဲ့အတွက် တိုသွားအောင် စာလုံး (၃၄) လုံးပဲပါပြီး ရိုက်ထည့်ရနည်းနည်းပိုလွယ်တဲ့ Address ဖြစ်အောင် ပြောင်းလိုက်တာလို့ မှတ်နိုင်ပါတယ်။ Address ကို ဒီထက် ထပ်တိုရင်တော့ သုံးတဲ့သူများလာတဲ့အခါ Address တွေ တိုက်ကုန်ပါလိမ့်မယ်။ ဒါကြောင့် ဒီထက်တော့ ထပ်တိုလို့ မရတော့ပါဘူး။

တစ်ကယ်တော့ အဲ့ဒါလည်း ရိုက်ထည့်ရ မလွယ်သေးပါဘူး။ Address မမှားချင်ရင် ကူးထည့်မှပဲ သေချာပါလိမ့်မယ်။ ဒါတောင် နှစ်ခါသုံးခါ သေချာပြန်စစ်ဖို့ လိုနိုင်ပါသေးတယ်။ လုံခြုံစိတ်ချရမှုအတွက် ဒီလောက်တော့ ဒုက္ခခံကြရပါလိမ့်မယ်။

လိုရင်းအနှစ်ချုပ်ကတော့ –

၁။ Public Key ကို ငွေပေးငွေယူ လက်ခံနိုင်တဲ့ အကောင့်သဖွယ်အသုံးပြုရတယ်။
၂။ အကောင့်လို့မခေါ်ကြဘဲ Address လို့ ခေါ်ကြတယ်။
၃။ Address တစ်ခုရဖို့အတွက် Public Key ကို တိုသွားအောင် Encode ထပ်လုပ်ရတယ်။
၄။ Address တစ်ခုဟာ ကိုယ်ပိုင်ဖြစ်ကြောင်း Private Key နဲ့ အတည်ပြု လက်မှတ်ထိုးပြရတယ်။

– လို့ မှတ်ရမှာပါ။

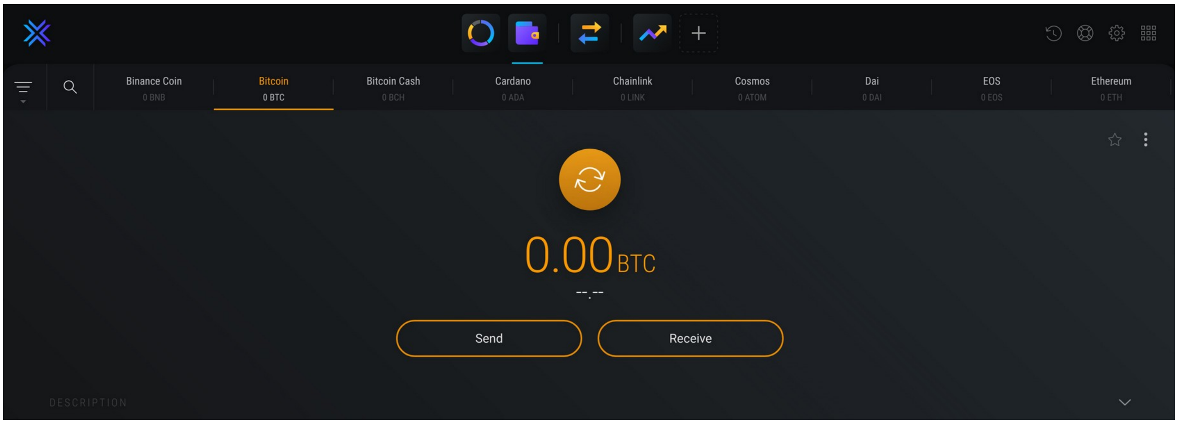
ဒီနေရာမှာ သတိပြုရမှာက လူတစ်ယောက်ကို Address တစ်ခုပဲ ကိုင်ခွင့်ရှိတာမျိုး မဟုတ်ပါဘူး။ ကြိုက်သလောက် Address တွေ ဖန်တီး အသုံးပြုခွင့်ရှိပါတယ်။ သုံးလည်း သုံးကြပါတယ်။ တစ်ခါသုံးလို မျိုးထိ သဘောထားကြပါတယ်။ Address တစ်ခုနဲ့ ငွေလက်ခံဖို့ အသုံးပြုပြီးရင် နောက်တစ်ကြိမ်အတွက် ထပ်မသုံးတော့ဘဲ နောက်ထပ် Address အသစ်ပြောင်းပြီး လက်ခံကြတာမျိုးတွေ ရှိပါတယ်။

Wallet

ဒီလိုမျိုး Address တွေရရှိဖို့အတွက် Key Pair တွေ ဖန်တီးတဲ့အလုပ်တွေ၊ Hash လုပ်တဲ့အလုပ်တွေ၊ သိမ်းဆည်းတဲ့အလုပ်တွေ၊ ငွေပေးငွေယူ လုပ်တော့မယ်ဆိုရင် Sign ထိုးတဲ့အလုပ်တွေကို ကိုယ်တိုင် လုပ်စရာမလိုပါဘူး။ အလုပ်လုပ်ပုံကို သိအောင်သာ ပြောပြနေတာပါ။ တစ်ကယ်တမ်း အဲ့ဒီအလုပ်တွေကို လုပ်ပေးနိုင်တဲ့ Wallet တွေကို အသုံးပြုကြရပါတယ်။ ဆော့ဖ်ဝဲ Wallet တွေရှိသလို၊ Hardware တွေလည်း ရှိပါတယ်။ Browser Extension အနေနဲ့လည်း ရှိသလို Mobile App အနေနဲ့လည်း ရှိပါတယ်။

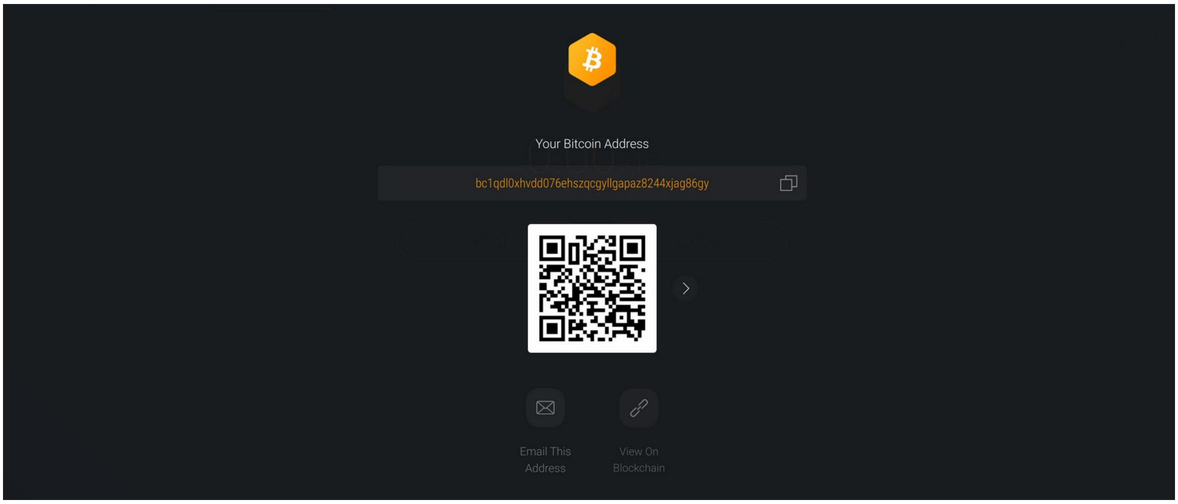
Wallet ထဲမှာ တစ်ကယ့် ငွေကြေး Data တွေ သိမ်းထားတာတော့ မဟုတ်ပါဘူး။ တစ်ကယ့် ငွေကြေး Data တွေက Network ထဲမှာပါ။ Wallet ထဲမှာ သိမ်းထားတာကတော့ အဲ့ဒီ Network ထဲက ကိုယ်ပိုင်တဲ့

ငွေကြေးကို ရယူအသုံးပြုလို့ရတဲ့ Private Key တွေကို စုပြီး သိမ်းထားပေးတာလို့ ဆိုနိုင်ပါတယ်။ ဒါတွေကို ပြောပြနေလို့သာ ရှုပ်တယ်ထင်ရပေမယ့် လက်တွေ့အသုံးပြုရတာ လွယ်ကူပါတယ်။ အခုပြောပြခဲ့တဲ့ သဘောသဘာဝတွေကို သိစရာမလိုဘဲ လူတိုင်းအသုံးပြုနိုင်ပါတယ်။ ပေးထားတဲ့ Screenshot ကို ကြည့်ပါ။

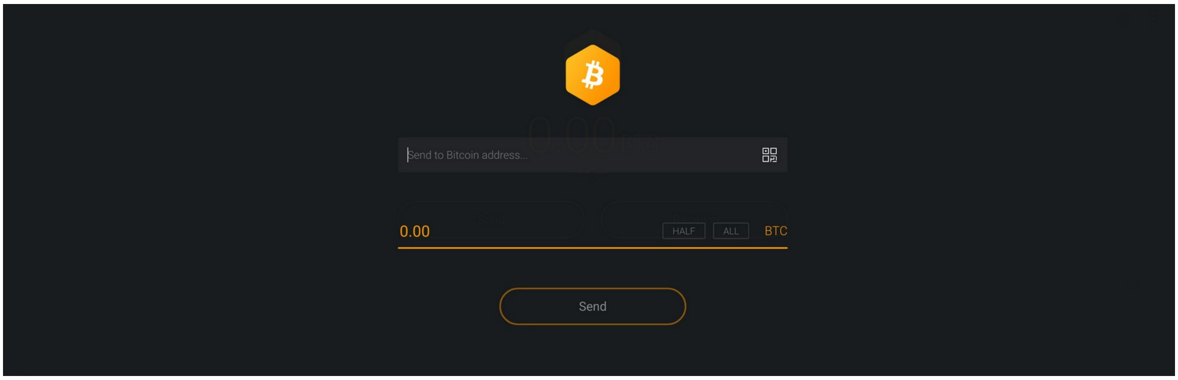


Exodus Cryptocurrency Wallet

ဒါဟာ Exodus လို့ခေါ်တဲ့ လူသုံးများတဲ့ Cryptocurrency Wallet ရဲ့ Desktop App ကို နမူနာပြထားတာပါ။ တစ်ကယ်တမ်း ငွေလက်ခံဖို့အတွက် ကိုယ့်ဘက်က Receive ဆိုတဲ့ ခလုပ်လေးကို နှိပ်လိုက်ယုံပါပဲ။ အခုလို Address တစ်ခုထွက်လာပါလိမ့်မယ်။



ဒါဟာ ကိုယ်ပိုင် Bitcoin Address တစ်ခုပါပဲ။ ဒီ Address ကို ငွေလွှဲပို့မယ့်သူထံ တစ်နည်းနည်းနဲ့ ပေးလိုက်ရင် ရပါပြီ။ ကိုယ့်ဘက်က ငွေလွှဲပို့ချင်ရင်လည်း Send ခလုပ်ကို နှိပ်လိုက်ယုံပါပဲ။ ပေါ်လာတဲ့ ဖောင်မှာ ပေးပို့လိုတဲ့ Address နဲ့ ငွေပမာဏကို ထည့်ပြီး ပို့လိုက်ရင် ရပါပြီ။



ဒါကြောင့် အလုပ်လုပ်ပုံကို နားလည်စေချင်လို့ ရှည်ရှည်ဝေးဝေးတွေ ရှင်းပြခဲ့ပေမယ့် လက်တွေ့အသုံးပြုမှုကတော့ အလွန်ရိုးရှင်း လွယ်ကူပါတယ်။ ဒီလို လွယ်ကူအောင် Wallet App တွေက လုပ်ပေးထားကြပါတယ်။ နမူနာပြခဲ့တဲ့ Exodus Wallet ကို Mobile App အနေနဲ့လည်း ထည့်သွင်းအသုံးပြုနိုင်ပါတယ်။ ဒီ လိပ်စာမှာ ကြည့်ပါ။

Exodus – https://exodus.com

တစ်ခြားအလားတူ Wallet App တွေအများကြီး ရှိပါသေးတယ်။ စမ်းသပ်လေ့လာနိုင်ဖို့အတွက် အသုံးပြုရလွယ်ကူပြီး လူသုံးများတဲ့ Wallet တချို့ကို ထည့်သွင်းဖော်ပြလိုက်ပါတယ်။

Trust Wallet – https://trustwallet.com
Atomic Wallet – https://atomicwallet.io
Coinomi – https://www.coinomi.com/en

ဒီ Wallet တွေအားလုံးကို မိုဘိုင်း App အနေနဲ့လည်း အသုံးပြုနိုင်တဲ့အတွက် သက်ဆိုင်ရာ App Store နဲ့ Play Store တို့မှာလည်း နာမည်နဲ့ ရှာဖွေပြီးတော့ ထည့်သွင်းအသုံးပြုနိုင်ပါတယ်။

သတိတော့ထားပါ။ ကိုယ်ပိုင်ဆိုင်သမျှအားလုံးက Wallet ထဲမှာမို့လို့ Wallet ပျောက်လို့တော့ မဖြစ်ပါဘူး။ ဖုန်းကျကွဲလို့ပဲဖြစ်ဖြစ်၊ Windows Crash ဖြစ်သွားလို့ပဲဖြစ်ဖြစ်၊ တစ်ခြား အကြောင်းကြောင့်ပဲ ဖြစ်ဖြစ် Wallet ပျောက်ရင် အကုန် ကုန်မှာပါ။ Backup တွေဘာတွေ လုပ်ထားလို့တော့ ရပါတယ်။ Restore Password တွေ ဘာတွေ ပေးထားလို့တော့ ရပါတယ်။ စမ်းသပ်ယုံဆိုရင် ကိစ္စမရှိပါဘူး။ အမှန်တစ်ကယ် အသုံးပြုတော့မယ်ဆိုရင်တော့ အဲ့ဒီလို Option တွေကို လေ့လာပြီး ကြိုတင်ပြင်ဆင်ထားဖို့ လိုပါလိမ့်မယ်။

တချို့ဆိုရင် Private Key တွေကို စာရွက်မှာချရေးပြီး မီးခံသတ္တာထဲမှာ ထည့်သိမ်းကြပါတယ်။ Private Key ရှိနေသ၍ Network ထဲက ငွေကို အချိန်မရွေး Access လုပ်လို့ရနိုင်တဲ့အတွက်ကြောင့်ပါ။

Hardware Wallet တွေလည်း ရှိပါသေးတယ်။ Key တွေကို USB Device လို Device ထဲမှာ သိမ်းလိုက်တာ မို့လို့ ကွန်ပျူတာမှာ ဗိုင်းရပ်ဝင်ပြီး Format ချလိုက်ရလို့ Wallet ပါသွားတယ် ဆိုတာမျိုး မဖြစ်တော့ပါဘူး။ ပိုပြီးတော့ လုံခြုံစိတ်ချရတယ်လို့ ဆိုကြပါတယ်။ Hardware Wallet တွေကို စာရေးသူကိုယ်တိုင် အသုံးပြု နေတာ မဟုတ်လို့ အသုံးပြုနည်းတော့ ထည့်မပြောပြနိုင်ပါဘူး။ စိတ်ဝင်စားရင် လေ့လာကြည့်နိုင်ဖို့ အတွက် လင့်တချို့ထည့်ပေးလိုက်ပါတယ်။ အမျိုးအစားနဲ့ မော်ဒယ်ပေါ်မူတည်ပြီး ဈေးနှုန်းကတော့ အမျိုး မျိုး ဖြစ်နိုင်ပါတယ်။

Ledger Hardware Wallet – https://www.ledger.com

Trezor Wallet – https://trezor.io

Cold Card Wallet – https://coldcardwallet.com

Bitcoin အချက်အလက်များ

Wallet တစ်ခုရွေးပြီးပြီဆိုရင် Bitcoin ကို စတင်အသုံးပြုဖို့အတွက် အသင့်ဖြစ်နေပါပြီ။ အထက်မှာပေးခဲ့တဲ့ နမူနာအများစုက နားလည်လွယ်အောင် Simplify လုပ်ပြီး ရှင်းပြခဲ့တဲ့ နမူနာတွေပါ။ ဒီလောက်ရှင်းအောင် ပြောတာတောင် အတော်ရှုပ်နေပြီလို့ထင်ပါတယ်။ တစ်ကယ့် Bitcoin ရဲ့ အချက်အလက်အသေးစိတ်တွေ သာ ထည့်ပြောရင် ပိုရှုပ်ကုန်မှာစိုး ထည့်မပြောဘဲ ချန်ထားခဲ့တာတွေ ရှိပါတယ်။ အဲ့ဒါတွေကို စုစည်းပြီး တော့ ပြောပြချင်ပါတယ်။

Encryption – Bitcoin က ECDSA လို့ခေါ်တဲ့ Encryption နည်းပညာကို အသုံးပြုပြီး SHA-256 လို့ခေါ်တဲ့ Hash Algorithm ကို အသုံးပြုပါတယ်။ Bitcoin Address တစ်ခုရဲ့ Private Key ကို ပိုင်ရှင်ဆီက တစ် နည်းနည်းနဲ့ တိုက်ရိုက်ခိုးယူရင်တော့ ရကောင်းရနိုင်ပါတယ်။ နည်းပညာအရ Crack လုပ်ပြီး ဖော်ယူလိုရင် တော့ ဖြစ်နိုင်ခြေရှိတဲ့ Key ကို တစ်ခုပြီးတစ်ခု ခန့်မှန်းရှာဖွေဖို့ နည်းလမ်းတစ်ခုသာ ရှိပါတယ်။ အဲ့ဒီလို ခန့်မှန်းရှာဖွေမယ်ဆိုရင် ရနိုင်ခြေဟာ 2^{256} ကြိမ်မှာ တစ်ကြိမ်သာ မှန်နိုင်ခြေရှိပါတယ်။ ဒါဟာ ပေါ့သေး သေး ကိန်းဂဏန်းမဟုတ်ပါဘူး။ ရေတွက်ပြလို့တောင် မရနိုင်လောက်အောင်ပါပဲ။ ဒီပမာဏကို **3Blue1Brown** လို့ခေါ်တဲ့ YouTube Channel တစ်ခုက မျက်စိထဲမြင်ကြည့်လို့ရအောင် တွက်ပြထားတာ စိတ်ဝင်စားစရာပါ။

လူတစ်ယောက်ကို ကွန်ပျူတာအလုံး (၄) ဘီလီယံစာ ပမာဏ တွက်ချက်နိုင်စွမ်းရှိတဲ့ စူပါကွန်ပျူတာ တစ် ယောက်တစ်လုံးရှိပြီး၊ ကမ္ဘာပေါ်မှာရှိတဲ့ လူပေါင်း (၄) ဘီလီယံက ဝိုင်းအဖြေရှာမယ်ဆိုရင်၊ ကမ္ဘာပေါင်း (၄) ဘီလီယံ ပါဝင်တဲ့၊ ဂလက်ဆီပေါင်း (၄) ဘီလီယံက နှစ်ပေါင်း (၁၀၀) ကျော်အဖြေရှာရင်တောင် အဖြေ မှန် ရနိုင်ခြေက (၄) ဘီလီယံမှာ (၁) ကြိမ်ပဲ ရှိတယ်လို့ တွက်ပြထားပါတယ်။ ဒီအတိုင်း ခန့်မှန်းအဖြေရှာဖို့ လုံးဝမဖြစ်နိုင်တဲ့ ပမာဏတစ်ခုပါ။ ဒီလိပ်စာမှာ လေ့လာကြည့်နိုင်ပါတယ်။

https://www.youtube.com/watch?v=S9JGmA5_unY

နောက်ပိုင်းမှာ ကနေ့ခေတ် ကွန်ပျူတာတွေနဲ့ ဘာမှမဆိုင်တော့လောက်အောင် စွမ်းဆောင်ရည် မြင့်မားလှ ပါတယ်ဆိုတဲ့ Quantum Computer တွေပေါ်လာရင်တော့ ဘယ်လိုဖြစ်လာမလဲ မသိပါဘူး။

Block Size – Bitcoin Blockchain မှာ ထည့်သွင်းသိမ်းဆည်းတဲ့ Block တစ်ခုရဲ့ အမြင့်ဆုံး Size ပမာဏကို 1 MB သတ်မှတ်ထားပါတယ်။ ဒါကြောင့် Block တစ်ခုကို Transaction ပေါင်း (၄,၀၀၀) ခန့်အထိ ထည့်သွင်းလို့ရပါတယ်။ သတိပြုပါ။ Transaction တစ်ခုကို Block တစ်ခုနှုန်းနဲ့ သိမ်းတာ မဟုတ်ပါဘူး။ Block တစ်ခုမှာ Transaction ပေါင်း (၄,၀၀၀) လောက် ဆန့်တဲ့အတွက် အဲ့ဒီပမာဏ အောက်မှာ ပါဝင်တဲ့ Transaction အရေအတွက်က ပြောင်းလဲနေပါတယ်။

Number of Blocks – ဒီစာကိုရေးသားနေချိန်မှာ Bitcoin Blockchain အတွင်း ရောက်ရှိနေတဲ့ နောက်ဆုံး Block ကတော့ (688,475) ဖြစ်ပါတယ်။ ဒါဟာ ပါဝင်တဲ့ Block အရေအတွက်ပါပဲ။ ဒီစာရင်းကို Blockchain Explorer မှာ အချိန်မရွေး လေ့လာကြည့်နိုင်ပါတယ်။

https://www.blockchain.com/explorer

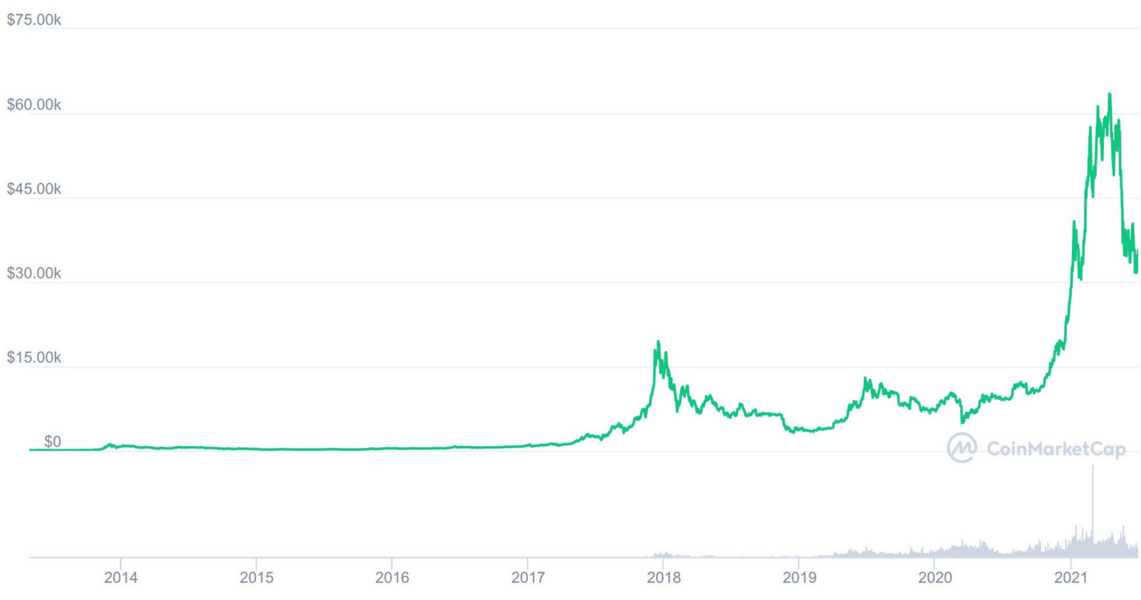
Blockchain Size – လက်ရှိ Bitcoin Blockchain ရဲ့ စုစုပေါင်း Size ပမာဏက 350 GB ကျော်ပါ။

Difficulty – Block အသစ်တစ်ခုကို ထည့်သွင်းနိုင်ဖို့အတွက် Proof of Work ကို ပြရတဲ့ ခက်ခဲမှုအဆင့်ဟာ ပုံသေမဟုတ်ပါဘူး။ ဝိုင်းပြီး တွက်တဲ့သူများရင်များသလို ခက်ခဲမှုအဆင့် ပိုမြင့်လာလေ့ရှိပါတယ်။ တွက်ချက်ရန်ကြာချိန် (၁၀) မိနစ်ခန့်မှာ ချိန်ညှိထားတာပါ။ ဒါကြောင့် တွက်တဲ့သူ ဘယ်လောက်များများ၊ ဘယ်လောက်မြန်မြန် Block တစ်ခုကို Bitcoin Blockchain မှာ ထည့်သွင်းနိုင်ဖို့အတွက် အချိန် (၁၀) မိနစ်ခန့် ကြာတယ်လို့ မှတ်သားရမှာ ဖြစ်ပါတယ်။

Reward – လက်ရှိ Block အသစ်ထည့်ပေးတဲ့အတွက် ထုတ်ပေးတဲ့ ဆုကြေးကတော့ 6.25 BTC ဖြစ်ပါတယ်။ စစချင်း ဆုကြေးက 50 BTC ပါ။ <u>Block ပေါင်း (၂၁၀,၀၀၀) ထည့်ပြီးတိုင်း ဆုကြေးကို တစ်ဝက်လျှော့ပါတယ်</u>။ ဒီသဘောသဘာဝကို Halving လို့ ခေါ်ကြပါတယ်။ (၃) ကြိမ် တစ်ဝက်လျှော့ခဲ့ပြီးပြီ မို့လို့ လက်ရှိဆုကြေးက 6.25 BTC ဖြစ်နေတာပါ။ ၂၀၂၄ ခုနှစ် ရောက်ရင် ဒီဆုကြေးကို ထက်ဝက် ထပ်လျှော့ဦးမှာပါ။

Max Supply – Bitcoin ရဲ့အမြင့်ဆုံးထုတ်ပေးမယ့် ကွိုင်အရေအတွက်က (၂၁) သန်း ဖြစ်ပါတယ်။ လက်ရှိ ဒီစာကို ရေးသားနေချိန်မှာ (၁၈.၇) သန်းကျော်ထိ ရှိနေပြီ ဖြစ်ပါတယ်။ Halving သဘောသဘာဝနဲ့ အသစ်ထုတ်ပေးတဲ့ ဆုကြေးကို လျှော့သွားမှာဖြစ်လို့ Coin အသစ်ထွက်တဲ့နှုံး နည်းသွားပါပြီ။ ၁၀ မိနစ်ကို Block အသစ်တစ်ခုနှုံးနဲ့ ပေးမယ့်ဆုကြေးကို တွက်လိုက်ရင် (၂၁) သန်းပမာဏကို ၂၁၄၀ ခုနှစ်ခန့်မှာ ပြည့်မယ်လို့ တွက်ချက်နိုင်ပါတယ်။ စာရေးသူကတော့ အသက် (၁၀၀) နေရရင်တောင် အဲ့ဒီပမာဏပြည့်တဲ့အချိန်ကို မီမှာ မဟုတ်တော့ပါဘူး။

Price – Bitcoin ရဲ့ လက်ရှိပေါက်စျေး 1 BTC ကို $30,000 အထက်၊ $40,000 အောက် ဖြစ်ပါတယ်။ အတိအကျကို မပြောတာက အချိန်နဲ့အမျှ စျေးနှုံး အမြဲပြောင်းလဲနေလို့ပါ။ ၂၀၁၁ ခုနှစ် ဧပြီလမှာ 1 BTC ကို $1 သာရှိခဲ့ပြီး၊ ၂၀၁၅ ခုနှစ် နှစ်ဦးပိုင်းမှာ 1 BTC ကို $300 ဝန်းကျင် ဖြစ်နေပါပြီ။ ၂၀၁၈ ခုနှစ် နှစ်ဦးပိုင်းမှာ 1 BTC ကို $13,600 ခန့်ထိ ဖြစ်ခဲ့ပြီး အမြင့်ဆုံးအနေနဲ့ ၂၀၂၁ ခုနှစ် ဧပြီလမှာ $63,000 ကျော်အထိ ရောက်ရှိခဲ့ပါတယ်။ အခုဒီစာရေးနေချိန်မှာ စျေးတွေ ပြန်ကျနေတာ ဖြစ်ပါတယ်။ ဒါဟာ စျေးကွက်ထဲမှာ လက်တွေ့ အရောင်းအဝယ် ပြုလုပ်နေကြတဲ့ ပမာဏတွေပါ။



Bitcoin Price History (USD) – CoinMarketCap

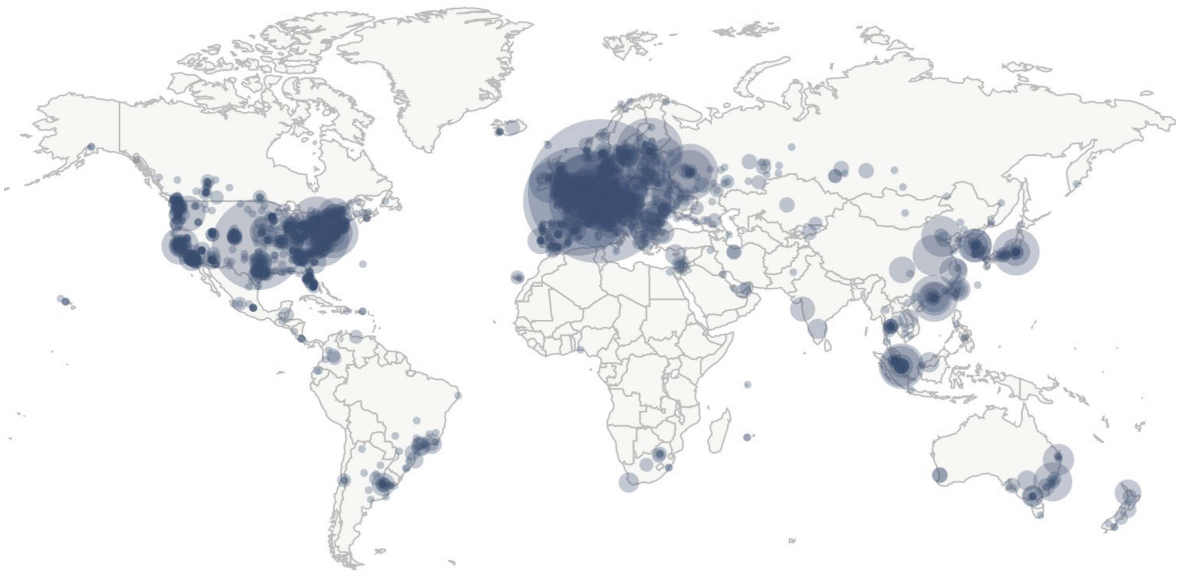
Market Cap – စုစုပေါင်းရှိနေတဲ့ Supply (၁၈) သန်းကျော်နဲ့ ဈေးကွက်ပေါက်ဈေးကို တွက်ချက်ကြည့်လိုက်ရင် Bitcoin ရဲ့ လက်ရှိ စုစုပေါင်း ဈေးကွက်တန်ဖိုး Market Cap ဟာ ဒေါ်လာ (၆၀၀) ဘီလီယံကျော်ထိ ရှိနေပြီဖြစ်ပါတယ်။ နှိုင်းယှဉ်ကြည့်မယ်ဆိုရင် ရွှေရဲ့ Market Cap ဟာ ဒေါ်လာ (၁၁) ထရီလီယံကျော်ဖြစ်ပြီး၊ အမေရိကန်ဒေါ်လာရဲ့ Market Cap ဟာ (၂၀) ထရီလီယံကျော် ဖြစ်ပါတယ်။ ဒီလင့်တွေမှာလေ့လာနိုင်ပါတယ်။

Cryptocurrency – https://coinmarketcap.com

Fiat Money – https://fiatmarketcap.com

Gold & Companies – https://8marketcap.com

Nodes – လက်ရှိဒီစာကိုရေးသားနေချိန် Bitcoin Network မှာ ပါဝင်တဲ့ စုစုပေါင်း Node အရေအတွက် (၁၀,၀၀၀) ကျော် ရှိပါတယ်။ Full Node ခေါ် Ledger မိတ္တူအပြည့်အစုံ ရှိတဲ့ Node တွေကို ပြောတာပါ။ အပြည့်အစုံမရှိတဲ့ Node တွေလည်း အများကြီးပါဝင်ပြီး၊ ထည့်ရေတွက်မထားပါဘူး။



Bitcoin Node များ၏ ကမ္ဘာအနှံ့ ဖြန့်ကျက်တည်ရှိမှု အခြေအနေ – bitnodes.io

Transaction Fee – Bitcoin နဲ့ ငွေပေးငွေယူ Transaction တစ်ခုကို ပြုလုပ်လိုက်တဲ့အခါ အဲ့ဒီ Transaction ကို တစ်ယောက်ယောက်က Proof of Work ပြုပြီး Confirm လုပ် ထည့်သွင်းပေးရပါတယ်။ ဒီလိုထည့်သွင်းပေးတဲ့အတွက် Coinbase ကနေ သတ်မှတ်ထားတဲ့ ပမာဏကို ဆုကြေးအနေနဲ့ ရတဲ့အပြင် Transaction Fee ကိုလည်း ရပါတယ်။ အပြင်မှာ ငွေလွှဲရင် ဘဏ်ကို လွှဲခပေးရသလိုပါပဲ။ Bitcoin နဲ့ ငွေလွှဲရင် Confirm လုပ်ပေးသူကို လွှဲခပေးရပါတယ်။ လွှဲခကို ကိုယ်တိုင်သတ်မှတ်လို့ ရပါတယ်။ ပုံမှန်အားဖြင့် မြန်မြန်လွှဲချင်ရင် လွှဲခများများ ပေးရပါတယ်။ ကိုယ့် Transaction အတွက် လွှဲခကို များများ သတ်မှတ်ပေးထားရင် Confirm လုပ်ပေးမယ့်သူတွေက ဦးစားပေးပြီး ထည့်ပေးနိုင်ခြေ ရှိလို့ပါ။ ပျမ်းမျှလွှဲခ ပမာဏဟာ အရောင်းအဝယ် ဈေးကွက် အရမ်းကောင်းနေစဉ်မှာ $60 ထိ ဖြစ်သွားခဲ့ဖူးပြီး၊ လက်ရှိဒီစာရေးသားနေချိန်မှာ $4 ဖြစ်ပါတယ်။

Satoshi (Unit) – Bitcoin တီထွင်သူကို ဂုဏ်ပြုတဲ့အနေနဲ့ Bitcoin ရဲ့ အသေးဆုံးသော ယူနစ်ပမာဏကို Satoshi လို့ခေါ်ကြပါတယ်။ 1 Satoshi ဟာ 0.00000001 BTC နဲ့ ညီမျှပါတယ်။

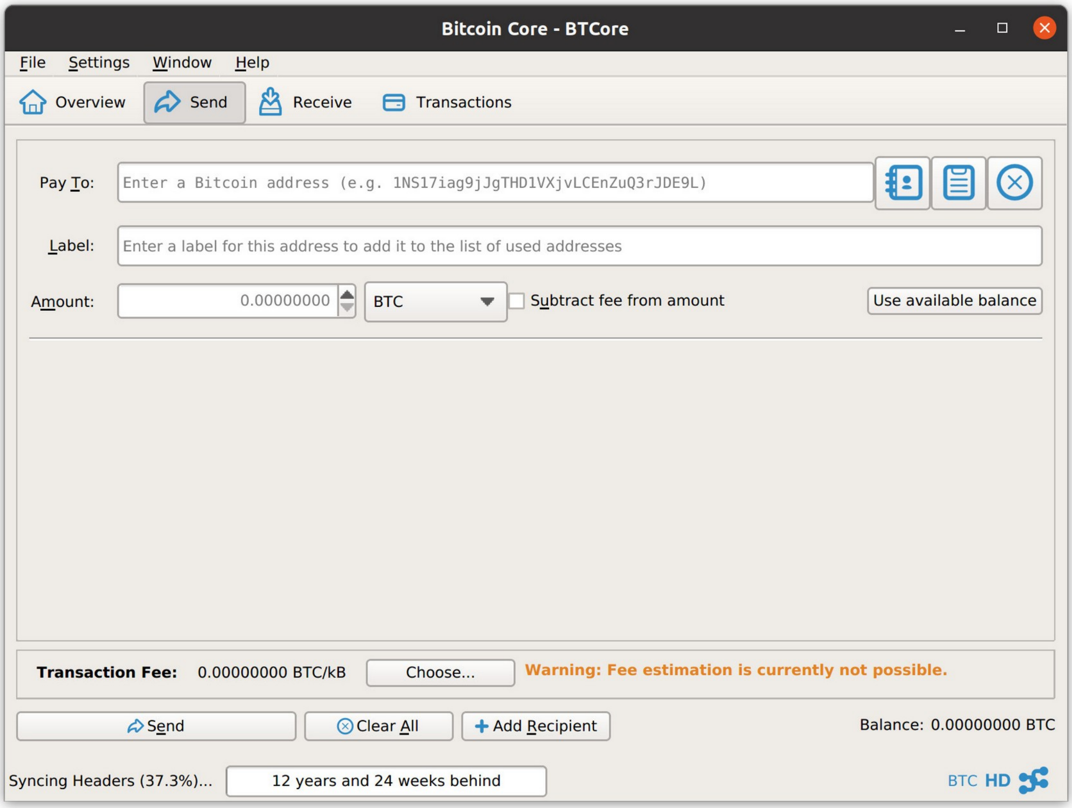
Airdrop – Cryptocurrency တစ်ခုအကြောင်းကို လူသိများစေလိုတဲ့အခါမှာ လူတွေစမ်းသပ်သုံးစွဲ ကြည့်လို့ ရနိုင်စေဖို့အတွက် အသေးဆုံးယူနစ် ပမာဏလေးတွေ ဖြန့်ဝေပေးကြလေ့ ရှိပါတယ်။ အဲ့ဒီလို ဖြန့်ဝေပေးတဲ့သဘောကို Airdrop လို့ ခေါ်ကြပါတယ်။ တန်ဖိုး သိပ်မရှိလှပေမယ့် လူတွေက Airdrop အနေနဲ့ လက်ခံရရှိတဲ့ Cryptocurrency တွေကို Wallet တွေထဲ ထည့်ကြ၊ စမ်းသပ်ပေးပို့ ကြည့်ကြတာမျိုးတွေ လုပ်လို့ရသွားပါတယ်။ စမ်းကြည့်ပြီး စိတ်ဝင်စားသွားခဲ့ရင် ဆက်လက် ပါဝင်လာလေမလားဆိုတဲ့ မျှော်မှန်းချက်နဲ့ပါ။ ဒါက Bitcoin နဲ့တိုက်ရိုက်သက်ဆိုင်တာ မဟုတ်ပါဘူး။ အကြောင်းတိုက်ဆိုင်လို့ သိသင့်တဲ့သဘောတစ်ခုအနေနဲ့ ထည့်ပြောလိုက်တာပါ။

Running a Full Node – ကိုယ်တိုင် Bitcoin Network မှာ Full Node အနေနဲ့ ပါဝင်ချင်ရင်လည်း ရပါတယ်။ Bitcoin Core ဆော့ဖ်ဝဲကို ကိုယ့်ကွန်ပျူတာမှာ Run ထားပေးယုံနဲ့ Full Node တစ်ခုဖြစ်နိုင်ပါတယ်။ ဒါပေမယ့် ဖြစ်နိုင်တယ်လို့ ပြောတာပါ။ အဲ့ဒီလို Full Node တစ်ခုအနေနဲ့ Run ဖို့အတွက် လိုအပ်မယ့် စက်စွမ်းအင်က မနည်းမနောပါ။ Blockchain တစ်ခုလုံးကို သိမ်းဆည်းဖို့အတွက် Storage အလုံအလောက် ရှိဖို့လိုသလို ကျန် Node တွေနဲ့ အမြဲဆက်သွယ် အလုပ်လုပ်နေနိုင်ဖို့ CPU စွမ်းအင်နဲ့ RAM လည်း အလုံအလောက် ရှိနေဖို့လိုအပ်ပါတယ်။ အင်တာနက်အဆက်အသွယ်လည်း ကောင်းရပါဦးမယ်။

Storage အလုံအလောက်ရှိပြီး စိတ်ဝင်စားရင် Bitcoin Core ကို Download ရယူပြီး စမ်းကြည့်ပါ။ Block တွေအကုန်မယူဘဲ နောက်ဆုံး (၂) နှစ်စာလောက်ပဲ ယူမယ်ဆိုရင်တော့ 8 GB လောက် Storage ရှိရင် စမ်းကြည့်လို့ရနိုင်ပါတယ်။

https://bitcoin.org/en/download

Bitcoin Core ဆော့ဖ်ဝဲကိုပဲ Wallet အနေနဲ့ အသုံးပြုရင်လည်း သုံးလို့ရနိုင်ပါတယ်။



Bitcoin Core

အခန်း (၄) – Mining, Exchanges နှင့် အထွေထွေ

Bitcoin Mining

Bitcoin နဲ့ပက်သက်ရင် ကြုံတွေ့ရတဲ့ အမေးအများဆုံး မေးခွန်းကတော့ Bitcoin ဘယ်လိုအလုပ်သလဲ မဟုတ်ပါဘူး။

၁။ Mine တူးတယ်ဆိုတာဘာလဲ။ နားမလည်ဘူး။
၂။ Mine တူးဖို့ ဘာဖြစ်လို့ စက်အကောင်းစား လိုတာလဲ။
၃။ Mine တူးလို့ လျှပ်စစ်စွမ်းအင်တွေ ကုန်တယ်လို့ ပြောကြတယ်၊ ဘာဖြစ်လို့လဲ။

– စသည်ဖြင့် အမေးများကြပါတယ်။ Bitcoin တစ်ကွိုင်ရဲ့တန်ကြေးက ဒေါ်လာသောင်းချီတန်ပြီး Mine တူးရင် Bitcoin တွေ ရတယ်ဆိုတော့ လိုချင်ကြတယ် ထင်ပါတယ်။ ရှေ့ပိုင်းမှာ ပြောခဲ့ပြီးသား ဆိုပေမယ့် ဒီ မေးခွန်းတွေရဲ့ အတိုချုပ်အဖြေကို ထပ်ပြောချင်ပါတယ်။

၁။ Mine တူးတယ်ဆိုတာ Proof of Work ကို ပြုပြီး Blockchain ထဲမှာ Transaction တွေကို ထည့်သိမ်းပေးခြင်းအားဖြင့် Coinbase ကနေ ဆုလာဒ်အဖြစ် Coin အသစ်တွေ ထပ်ထွက်လာအောင် တူးယူတာပါ။

၂။ Proof of Work ဆိုတာ လွယ်လွယ်ပြောရရင် ခက်ခဲတဲ့ ပုစ္ဆာတစ်ပုဒ်ကို တွက်ပြရတာလို့ ပြောကြပါတယ်။ အခုဒီစာအုပ်ကို ဖတ်နေသူတွေကတော့ သိနေကြပါပြီ။ Proof of Work ပုစ္ဆာဆိုတာ သတ်မှတ်ထားတဲ့ Hash အမှန်ကို ရအောင် ရှာဖွေပေးရတာပါ။ ဒီလိုရှာဖွေဖို့အတွက် စွမ်းဆောင်ရည်မြင့်တဲ့ ကွန်ပျူတာ

လိုပါတယ်။ ကိုယ့်ကွန်ပျူတာက သူများကွန်ပျူတာထက် စွမ်းဆောင်ရည် ပိုကောင်းမှသာ သတ်မှတ်ထားတဲ့ Hash ကို သူများအရင် တွေ့နိုင်ခြေ ပိုများတာပါ။ ဒါကြောင့် Mine တူးဖို့အတွက် စက်အကောင်းစား လိုတယ်လို့ ပြောကြတာပါ။

၃။ ဒီလိုကွန်ပျူတာနဲ့ စက်အကောင်းစားတွေ အပြိုင်အဆိုင်တပ်ဆင်ပြီး Mine တွေတူးကြတဲ့အတွက် လျှပ်စစ်စွမ်းအင် ကုန်နေတယ်လို့ ပြောတာပါ။ စက်ဖွင့်လို့ မီးအားကုန်တာက တစ်ကယ်တော့ မထူးဆန်းပါဘူး။ ကုန်မှာပါပဲ။ ဒါပေမယ့် ဒါကို ပြဿနာတစ်ရပ်အနေနဲ့ ပြောကြတာကတော့၊ တချို့က Bitcoin ကို တန်ဖိုးအစစ်အမှန်မရှိတဲ့ အကျိုးမဲ့ ဖြုန်းတီးမှုတစ်ခုလို့ မြင်နေကြဆဲပါပဲ။ ဒါကြောင့် အကျိုးမရှိတဲ့အလုပ်တွေကို လုပ်နေပြီး မီးအားတွေ အလကားဆုံးရှုံးနေတယ်ဆိုတဲ့ အမြင်နဲ့ ပြောနေကြတာပါ။ ဒီအကြောင်းကို ခဏနေတော့ Bitcoin ရဲ့ အားနည်းချက်များအကြောင်း ပြောတဲ့အခါ ထပ်ပြောပါဦးမယ်။

Bitcoin အပါအဝင် Cryptocurrency တွေ Mine လုပ်ဖို့အတွက် Miner ဆော့ဖ်ဝဲတွေရှိသလို သူများတွေ တူးနေကြပြီး ကိုယ်လည်းဝင်တူးလို့ရတဲ့ Mining Pool တွေလည်း ရှိပါတယ်။ အဲ့ဒီဆော့ဖ်ဝဲတွေအကြောင်း မပြောခင် Mine လုပ်တဲ့အခါ သွားရတဲ့ အဆင့်တွေကို အရင်ပြောပြချင်ပါတယ်။

၁။ Bitcoin ကို အသုံးပြုပြီး ငွေပေးငွေယူ Transaction တွေ လုပ်ကြတဲ့အခါ Blockchain ထဲကို ထည့်ပြီး Confirm မလုပ်ရသေးတဲ့ Pending Transaction တွေရှိနေမှာပါ။ Network ထဲမှာ အဲ့ဒီ Transaction တွေကို Transaction Pool အနေနဲ့ ထားပါတယ်။

၂။ Block အသစ်တစ်ခုတည်ဆောက်ပြီး Data အနေနဲ့ Transaction Pool ထဲကနေ ဆန့်သလောက် Transaction တွေကိုရယူပြီး အဲ့ဒီ Block ထဲကို ထည့်ရပါတယ်။

၃။ ထည့်ထားတဲ့ Transaction တွေဟာ မှန်ကန်မှုရှိမရှိ စစ်ဆေးရပါတယ်။ Blockchain ထဲမှာ နောက်ကြောင်းပြန် လိုက်ပြီး လွှဲပို့သူမှာ သူလွှဲပို့လိုတဲ့ငွေ တစ်ကယ်ရှိမရှိ စစ်ရတာမျိုးပါ။

၄။ ပြီးတဲ့အခါ သတ်မှတ်ထားတဲ့ Hash ကို စတွက်ရပါတယ်။ ရလဒ် Hash ရဲ့ ရှေ့ဆုံးက သုည ဘယ်နှစ်လုံးနဲ့ စရမှာလည်းဆိုတဲ့ Difficulty ကို Network က သတ်မှတ်ထားတဲ့အတိုင်း ရအောင် Nonce တန်ဖိုးတွေ တစ်ခုပြီးတစ်ခု ပြောင်းထည့်ကြည့်ပြီး နောက်ဆုံးအဖြေမှန်တဲ့အထိ တွက်ယူရမှာပါ။

၅။ အဖြေမှန်ရပြီဆိုရင် Block ကို တွက်ချက်ရရှိလာတဲ့ Nonce တန်ဖိုးနဲ့အတူ ကိုယ့်စက်ထဲက Blockchain ထဲမှာ ထည့်ပေးလိုက်လို့ရပါပြီ။ ဒီလိုထည့်ပေးလိုက်တဲ့ ရလဒ်ကို Network ထဲမှာ Broadcast လုပ်ပေးလိုက်ရင် ကျန် Node တွေကလည်း ကူးယူထည့်သွင်းသွားမှာပါ။

၆။ ဒီလို Block အသစ်တစ်ခုကို ထည့်သွင်းပေးလိုက်နိုင်တဲ့အခါ သတ်မှတ်ထားတဲ့ ဆုကြေးနဲ့ Transaction Fee တို့ကို ထည့်ပေးသူက ရရှိမှာဖြစ်ပါတယ်။ လက်ရှိဒီစာရေးနေချိန်မှာ ဆုကြေးအဖြစ် 6.25 BTC ကို ရရှိမှာဖြစ်ပြီး Transaction Fee ကတော့ Block ထဲမှာ ထည့်သွင်းပေးလိုက်တဲ့ Transaction တွေပေါ်မှာ မူတည်ပါတယ်။ ပုံသေရှိမှာ မဟုတ်ပါဘူး။

ထုံးစံအတိုင်း ဒီအလုပ်တွေကို ကိုယ်တိုင် လုပ်စရာမလိုပါဘူး။ လုပ်ပေးနိုင်တဲ့ Miner ဆော့ဖ်ဝဲတွေ ရှိပါတယ်။ ဒါပေမယ့် ပြဿနာက၊ ကနေ့ခေတ်မှာ အိမ်သုံးကွန်ပျူတာနဲ့ Bitcoin Mine တူးတာဟာ ဘာအဓိပ္ပါယ်မှ မရှိတော့ပါဘူး။ သူများတွေက ဒီလို Mine တူးဖို့အတွက် သီးခြားတီထွင်ထားတဲ့ စက်ကြီးတွေနဲ့ တူးနေချိန်မှာ ကိုယ့်အိမ်ကကွန်ပျူတာမှာ ဘယ်လောက်ကောင်းတဲ့ စက်ပစ္စည်းတွေပဲ တပ်ထားပါစေ၊ သူတို့နဲ့ပြိုင်ပြီး တူးနိုင်ဖို့ဆိုတာ မဖြစ်နိုင်သလောက် ဖြစ်နေပါပြီ။

ဒါပေမယ့် Cryptocurrency ဆိုတာ Bitcoin တစ်မျိုးထဲရှိတာ မဟုတ်ပါဘူး။ တစ်ခြား Cryptocurrency တွေကို တူးယူပြီး Bitcoin နဲ့ ပြန်လဲယူလို့ ရနိုင်ပါတယ်။ ဒီလိုတူးယူတဲ့အခါမှာလည်း တစ်ယောက်ထဲ၊ ကိုယ့်စက်တစ်လုံးထဲ တူးလို့ကတော့ ရနိုင်မှာ မဟုတ်ပါဘူး။ သူများတွေက စက်တွေအများကြီး ပေါင်းစပ်ပါဝင်တဲ့ Mining Pool တွေဖန်တီးပြီး တူးယူနေကြတာပါ။ ဒါပေမယ့် ကိုယ်ကလည်း အဲ့ဒီ Mining Pool တွေမှာ ဝင်ပါလို့တော့ ရနိုင်ပါတယ်။ ရလာတဲ့ ဆုကြေးကို Pool မှာ ပါဝင်သူတွေ ခွဲဝေပေးလို့ ကိုယ့်စက်ရဲ့ စွမ်းအင်ပေါ်မူတည်ပြီး ဝေစုကိုရရှိမှာ ဖြစ်ပါတယ်။

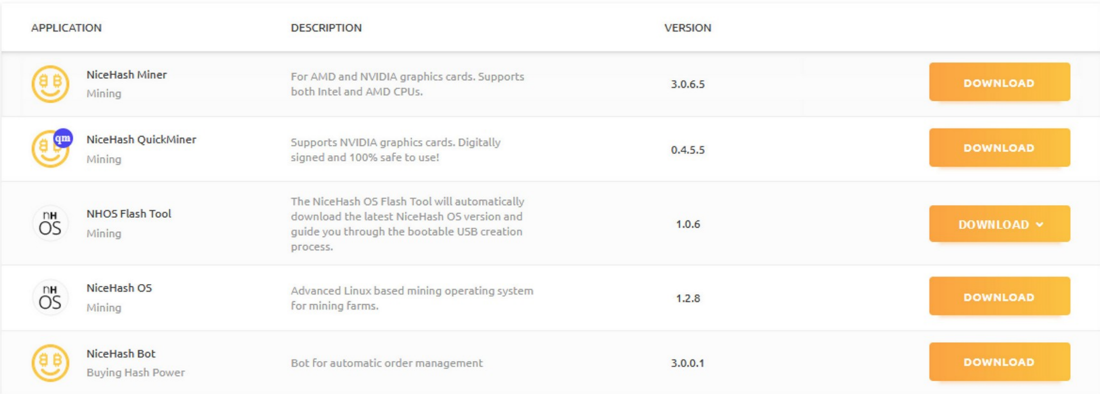
ဒါကိုစိတ်ဝင်စားလို့ စမ်းကြည့်ချင်ရင်တော့ NiceHash လို့ခေါ်တဲ့ နည်းပညာနဲ့ စမ်းကြည့်နိုင်ပါတယ်။ ဒီလိပ်စာမှာ ကြည့်ပါ။

https://www.nicehash.com

ကျန်တာ ဘာမှမလုပ်ခင် Register လုပ် အကောင့်ဆောက်ပြီး Login ဝင်ထားလိုက်ပါ။ ဘယ်လို Register

လုပ်ရလဲဆိုတာမျိုးထိတော့ ထည့်မပြောတော့ပါဘူး။ ကိုယ်တိုင်စမ်းကြည့်လိုက်ပါ။ Register လုပ်ရ မခက်ပါဘူး။ ပြီးတဲ့အခါ လိုအပ်တဲ့ ဆော့ဖ်ဝဲကို ဒီလိပ်စာကနေ Download ယူနိုင်ပါတယ်။

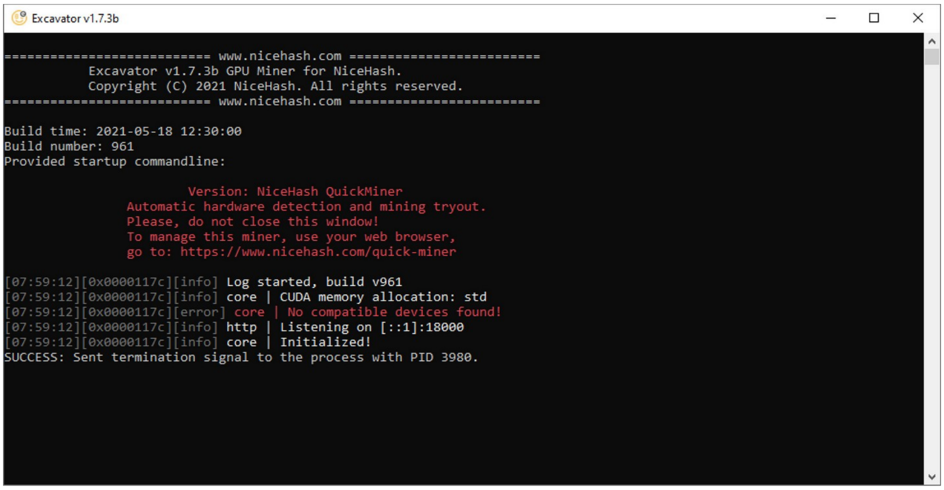
https://www.nicehash.com/download-center



APPLICATION	DESCRIPTION	VERSION	
NiceHash Miner Mining	For AMD and NVIDIA graphics cards. Supports both Intel and AMD CPUs.	3.0.6.5	DOWNLOAD
NiceHash QuickMiner Mining	Supports NVIDIA graphics cards. Digitally signed and 100% safe to use!	0.4.5.5	DOWNLOAD
NHOS Flash Tool Mining	The NiceHash OS Flash Tool will automatically download the latest NiceHash OS version and guide you through the bootable USB creation process.	1.0.6	DOWNLOAD
NiceHash OS Mining	Advanced Linux based mining operating system for mining farms.	1.2.8	DOWNLOAD
NiceHash Bot Buying Hash Power	Bot for automatic order management	3.0.0.1	DOWNLOAD

NiceHash Download Center

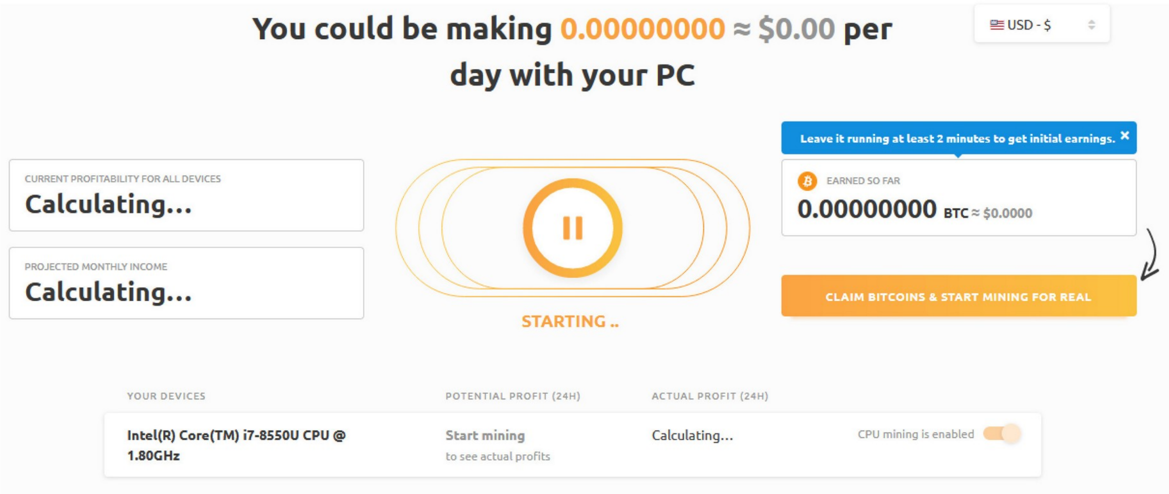
စမ်းကြည့်ဖို့ အမြန်ဆုံးကတော့ NiceHash QuickMiner ပါပဲ။ Windows မှာပဲ သုံးလို့ရပါတယ်။ Mac တို့ Linux တို့မှာ မရပါဘူး။ ဘာမှလုပ်စရာ မလိုပါဘူး၊ Download လုပ်ပြီး Run ထားလိုက်ရင်ရပါပြီ။ အခုလို မျိုး Terminal Window လေးတစ်ခုကို တွေ့ရပါလိမ့်မယ်။



NiceHash QuickMiner

အဲ့ဒီ Terminal လေးကို မပိတ်ဘဲ ဖွင့်ထားလိုက်ရင် သူ့ဘာသာ စပြီးတော့ Mine လုပ်နေပါပြီ။ Mine လုပ်လို့ရတဲ့ ရလဒ်ကို သိချင်ရင်တော့ ဒီလိပ်စာမှာ ဝင်ကြည့်ရပါတယ်။

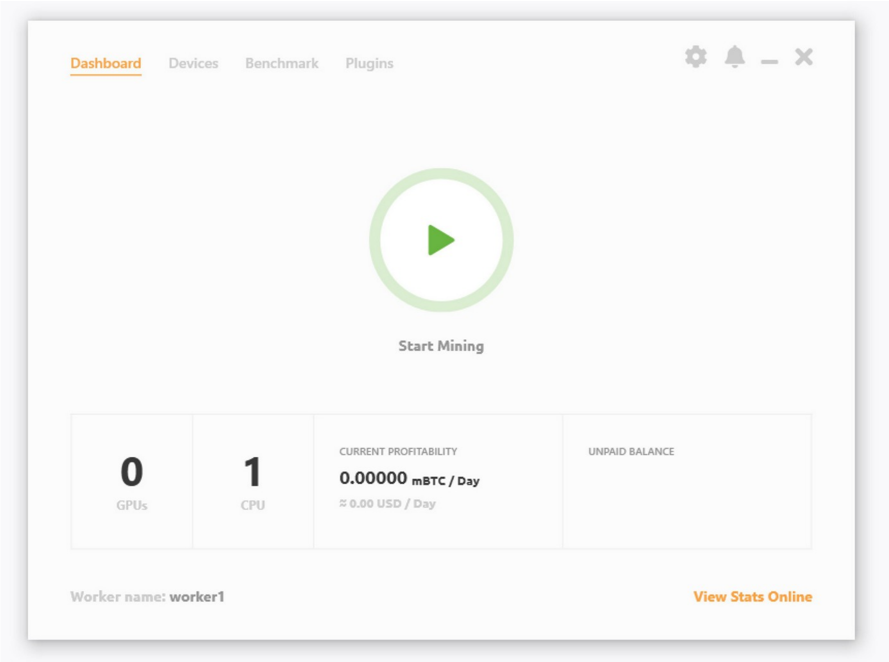
https://www.nicehash.com/quick-miner



ဒါက စမ်းကြည့်ဖို့ အလွယ်ဆုံးနဲ့ အမြန်ဆုံးနည်းကို ပြောတာပါ။ NiceHash က ကိုယ့်ကွန်ပျူတာကို သူ့ရဲ့ Mining Pool ထဲမှာ ထည့်အလုပ်လုပ် ပေးသွားတဲ့သဘောပါ။

Mining Pool ဆိုတာ Proof of Work အတွက် လိုအပ်တဲ့ Hash ကို လူခွဲပြီး အဖြေရှာလိုက်တဲ့ သဘောမျိုးပါ။ ဥပမာ – အဖြေမှန်ရဖို့ အကြိမ် (၁) သန်း Hash လုပ်ရမယ်ဆိုရင်၊ ကွန်ပျူတာ တစ်လုံးထဲက အကြိမ် (၁) သန်းလုံးကို မလုပ်ဘဲ၊ ၁ ကနေ ၁ သိန်းထိ တစ်ယောက်လုပ်၊ ၁ သိန်းကနေ ၂ သိန်းထိ နောက်တစ်ယောက်လုပ်၊ စသည်ဖြင့် ကွန်ပျူတာ (၁၀) လုံးလောက် ခွဲပြီး အလုပ်လုပ်လိုက်မယ်ဆိုရင် အဖြေရတာ (၁၀) ဆ ပိုမြန်သွားမှာပါ။ ဒီလိုပေါင်းလုပ်ကြတဲ့ သဘောမျိုးပါ။

အမြန်စမ်းကြည့်ယုံမဟုတ်ဘဲ အမြဲလုပ်ချင်ရင်တော့ NiceHash QuickMiner ကို မသုံးဘဲ ရိုးရိုး NiceHash Miner ကိုအသုံးပြုနိုင်ပါတယ်။ NiceHash Miner က ကိုယ့်အတွက် Bitcoin Address တစ်ခုကို Mining Address တစ်ခုအနေနဲ့ ပေးထားမှာပါ။ ထုတ်ယူချင်တဲ့အခါ အဲ့ဒီ Address ကနေ နောက်ပိုင်းမှာ ကိုယ့်ကိုယ်ပိုင် Wallet Address ကို ပြောင်းပို့ထားလို့ရပါတယ်။



NiceHash Miner

ရမယ့် ဝေစုဆုငွေ ပိုလိုချင်ရင်တော့ ရိုးရိုးကွန်ပျူတာနဲ့ မလုံတော့ပါဘူး။ စွမ်းဆောင်ရည်ကောင်းတဲ့ GPU တွေ တပ်ဆင်ထားဖို့ လိုပါလိမ့်မယ်။

ဥပမာ – ရိုးရိုး Intel Core i7 လို CPU ရဲ့ SHA-256 Hash Rate က 11 Mh/s ဝန်းကျင်မှာ ရှိလို့ တစ်စက္ကန့်ကို အကြိမ် (၁၁) သန်းလောက် Hash လုပ်နိုင်စွမ်းရှိတယ်ဆိုတဲ့ သဘောပါ။ Nvidia GTX 480 လို GPU မျိုးဆိုရင် Hash Rate က 140 Mh/s လောက်ထိ ရှိပါတယ်။ အတော်ကွာသွားပါပြီ။ ဒါက ရှာဖွေတွေ့ရှိရတဲ့ Update မဖြစ်တဲ့ အချက်အလက်အဟောင်းပေါ်မှာ အခြေခံထားတာ ဖြစ်ပြီး Bitcoin ကအသုံးပြုထားတဲ့ SHA-256 အတွက်ပဲ ပြောတာပါ။ SHA-256 ကို မသုံးတဲ့ တစ်ခြား Cryptocurrency တွေအတွက်ဆိုရင်တော့ Hash Rate က တူမှာ မဟုတ်တော့ပါဘူး။ ဒါကြောင့် ပုံသေမမှတ်ဖို့တော့ လိုပါတယ်။

အဓိကကျတဲ့ မှတ်သားစရာကတော့ Hash လုပ်ပြီး အဖြေရှာတဲ့ အလုပ်မျိုးမှာ GPU က CPU ထက် အဆပေါင်းများစွာ ပိုမြန်တယ်ဆိုတဲ့အချက်ပါပဲ။ Bitcoin မဟုတ်တဲ့ တစ်ခြား Cryptocurrency တွေကလည်း Mine တူးဖို့အတွက် GPU တွေနဲ့တူးရတာ ပိုအဆင်ပြေအောင် ဒီဇိုင်းလုပ်ထားတတ်ကြပါတယ်။ ဒီအကြောင်းကို နောက်မှ Ethereum အကြောင်းပြောတဲ့အခါ အကြမ်းဖျင်း ထည့်ပြောပြပါမယ်။

လိုရင်းကတော့ ရလဒ်ကောင်းလိုချင်ရင်တော့ ကိုယ့်ကွန်ပျူတာမှာ စွမ်းဆောင်ရည်ကောင်းတဲ့ GPU တွေ ထပ်တပ်ဖို့ လိုမယ်လို့ ဆိုလိုတာပါ။ ကိုယ့်ကွန်ပျူတာက ထွက်ပေးနိုင်တဲ့ပမာဏ ပိုလာတာနဲ့အမျှ ရမယ့် ဝေစုလည်း ပိုလာမှာပါ။ NiceHash က စက်မှာတပ်ဆင်ထားတဲ့ CPU တွေ GPU တွေ အကုန်လုံးကို အသုံးပြုပြီး အလုပ်လုပ်ပေးနိုင်ပါတယ်။

ကနေ့အချိန်မှာ အိမ်သုံးကွန်ပျူတာနဲ့ Bitcoin Mine တူးတာဟာ ဘာအဓိပ္ပါယ်မှ မရှိတော့ဘူးလို့ ပြောခဲ့ပါတယ်။ ဘာဖြစ်လို့လဲဆိုတော့၊ တစ်ကယ့် Miner တွေက Bitcoin Mine တူးဖို့အတွက် သီးသန့်တီထွင်ထားတဲ့ ASIC ခေါ် စက်တွေကို သုံးနေကြလို့ပါ။ ASIC ဆိုတာ Application-Specific Integrated Circuit ရဲ့ အတိုကောက်ပါ။ ကွန်ပျူတာလို ဘက်စုံ သုံးလို့မရပါဘူး။ သတ်မှတ်ထားတဲ့ အလုပ်တစ်ခုကိုပဲ သီးသန့် လုပ်တာမို့လို့ ပိုပြီးတော့ ထိထိရောက်ရောက် အလုပ်လုပ်နိုင်ပါတယ်။

ဥပမာ – လက်ရှိပေါက်ဈေး ဒေါ်လာ (၂၀,၀၀၀) ကျော် တန်ကြေးရှိတဲ့ AntMiner S19 Pro လို ASIC စက်မျိုးဆိုရင် SHA-256 အတွက် Hash Power က 110 Th/s ထိရှိပါတယ်။ စောစောကပြောခဲ့တဲ့ Nvidia GTX 480 ရဲ့ 140 Mh/s ဆိုတာနဲ့ယှဉ်ရင် တော်တော်ကြီးကို ကွာခြားသွားပါပြီ။ Mh/s ဆိုတာ Mega Hash per Second ရဲ့ အတိုကောက်ပါ။ အခုက သူ့ထက်မြင့်တဲ့ Giga Hash per Second (Gh/s) တောင် မဟုတ်တော့ပါဘူး။ Tera Hash per Second (Th/s) ထိ ဖြစ်နေပါပြီ။

https://shop.bitmain.com/release/AntminerS19Pro/overview

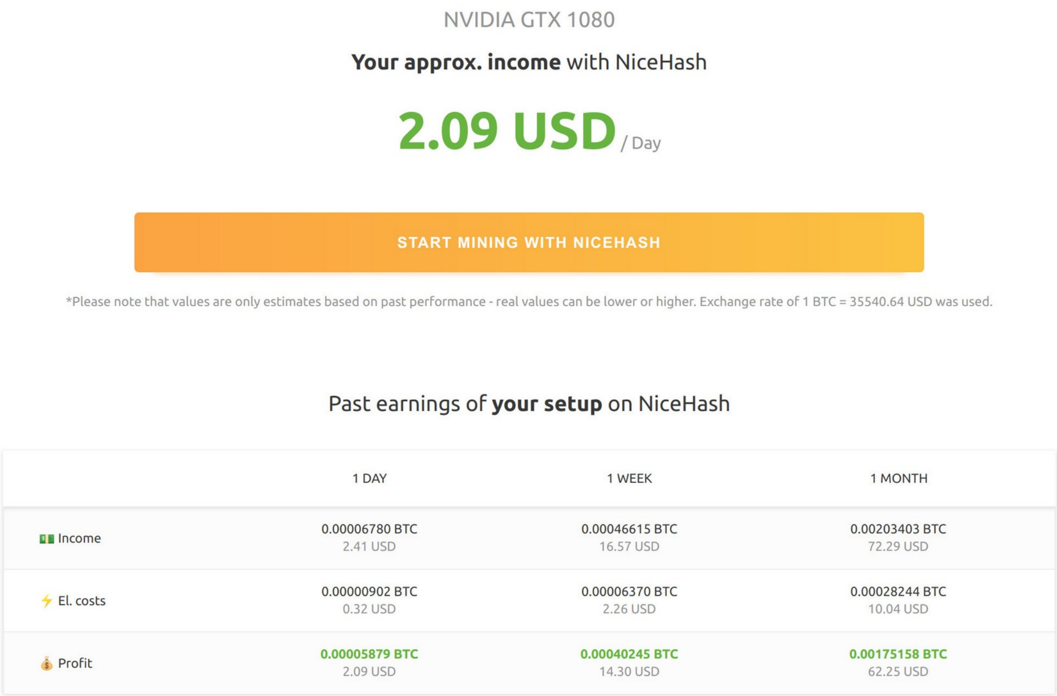
ပြီးတော့ ဒီလိုစက်မျိုးတွေကိုမှ တစ်လုံးနှစ်လုံး မဟုတ်ပါဘူး၊ စက်တွေအများကြီးနဲ့ Mining Firm တွေ ထူထောင်ပြီးတော့ တူးကြတာပါ။ တရုတ်ပြည် အရှေ့မြောက်ပိုင်းက စက်ရုံဟောင်းတစ်လုံးကို ပြန်ပြင်ပြီး တည်ထောင်ထားတဲ့ Mining Firm တစ်ခုရဲ့ Hash Rate ဆိုရင် 360,000 TH/s ပမာဏထိ ရှိနေပြီး တစ်လ ဝင်ငွေ 700 BTC လောက်ထိ ရနေတယ်လို့ သိရပါတယ်။

တရုတ်နိုင်ငံ၊ အတွင်းမွန်ဂိုလီးယားရှိ Bitcoin Mining Firm တစ်ခု – Photo: Stefen Chow

ဒီလို Mining Firm တွေရှိနေလို့ ဘယ်လောက်ကောင်းတဲ့ GPU ကိုပဲ သုံးသုံး သူတို့နဲ့ ယှဉ်ပြိုင်ပြီး တူးနိုင်ဖို့ မလွယ်ဘူးလို့ ဆိုတာပါ။ ဒါပေမယ့် လုံးဝမရနိုင်တော့တာတော့ မဟုတ်ပါဘူး။ အထက်မှာပြောခဲ့သလို တစ်ခြား Cryptocurrency ကို Mining Pool တွေမှာဝင်တူးပြီး ဆုငွေဝေစုတော့ ရနိုင်ပါသေးတယ်။ NiceHash ကလည်း အဲ့ဒီလိုသဘောမျိုးပါပဲ။ ဆုငွေကို BTC နဲ့ ထုတ်ပေးပေမယ့် တစ်ခြား Cryptocurrency အတွက် ဆုငွေကို BTC ပြောင်းပြီးမှ ပြန်ပေးတာမို့လို့ပါ။ သူက Bitcoin တူးပေးနေတာမျိုးတော့ ဟုတ်ချင်မှ ဟုတ်ပါလိမ့်မယ်။

ဒီနည်းနဲ့ ကိုယ့်စက်အမျိုးအစားပေါ်မူတည်ပြီး တစ်နေ့ခန့်မှန်းဝင်ငွေ ဘယ်လောက်ရှိနိုင်သလဲဆိုတာ ဒီနေရာမှာ တွက်ကြည့်လို့ ရပါတယ်။

https://www.nicehash.com/profitability-calculator



	1 DAY	1 WEEK	1 MONTH
Income	0.00006780 BTC 2.41 USD	0.00046615 BTC 16.57 USD	0.00203403 BTC 72.29 USD
El. costs	0.00000902 BTC 0.32 USD	0.00006370 BTC 2.26 USD	0.00028244 BTC 10.04 USD
Profit	0.00005879 BTC 2.09 USD	0.00040245 BTC 14.30 USD	0.00175158 BTC 62.25 USD

Estimate Earning – Nvidia GTX 1080

ဒါမှမဟုတ် စက်ဝယ်ချင်လို့ ဘယ်လိုစက်အမျိုးအစားဆိုရင် ဘယ်လောက်ဝင်နိုင်သလဲဆိုတာကို သိချင်ရင် ဇယားနဲ့ နှိုင်းယှဉ်ပြထားတာကို ဒီနေရာမှာကြည့်လို့ရပါတယ်။

https://www.nicehash.com/mining-hardware

ASIC | **GPU** | CPU

MODEL	NHQM	NHM	NHOS	DAILY EARNINGS	EL. COST	POWER USAGE	EFFICIENCY	NET PROFIT
NVIDIA Tesla A100	✓			11.05 USD	- 0.48 USD	200 W	0.0553 USD/watt	10.57 USD/day
NVIDIA RTX 3090	✓	✓	✓	7.78 USD	- 0.68 USD	285 W	0.0273 USD/watt	7.10 USD/day
NVIDIA RTX 3080	✓	✓	✓	6.22 USD	- 0.53 USD	220 W	0.0283 USD/watt	5.69 USD/day
AMD Radeon VII		✓	✓	5.86 USD	- 0.7 USD	290 W	0.0202 USD/watt	5.16 USD/day
NVIDIA A40	✓			5.40 USD	- 0.46 USD	190 W	0.0284 USD/watt	4.94 USD/day
NVIDIA TITAN V	✓	✓	✓	5.08 USD	- 0.38 USD	160 W	0.0318 USD/watt	4.70 USD/day
NVIDIA RTX 3080 Ti	✓	✓		5.08 USD	- 0.67 USD	280 W	0.0182 USD/watt	4.41 USD/day
NVIDIA RTX 2080 Ti	✓	✓	✓	4.23 USD	- 0.35 USD	145 W	0.0292 USD/watt	3.88 USD/day
NVIDIA TITAN RTX	✓	✓	✓	4.34 USD	- 0.6 USD	250 W	0.0173 USD/watt	3.74 USD/day
AMD RX 6800 XT 16GB		✓		4.19 USD	- 0.46 USD	190 W	0.0221 USD/watt	3.73 USD/day

Earning Estimate by Hardware

ဒီနေရာမှာ ဘယ်လိုစက်မျိုးကို ဝယ်တာ ကိုယ့်အတွက် အသင့်တော်ဆုံးဖြစ်မယ်၊ အမြင့်ဆုံးစွမ်းဆောင်ရည်ရအောင် Overclock တွေဘာတွေ ဘယ်လိုလုပ်ရတယ်၊ အကောင်းဆုံး ရလဒ်ရဖို့အတွက် Setting တွေ ဘယ်လိုချိန်သင့်တယ် စသည်ဖြင့် ပြောစရာတွေ အများကြီးရှိလာပါလိမ့်မယ်။ ဒါတွေကတော့ Bitcoin ရဲ့ အလုပ်လုပ်ပုံနဲ့ တိုက်ရိုက် မသက်ဆိုင်တော့ဘဲ၊ ကွန်ပျူတာ Hardware ကို ထိရောက်အောင် စီမံတဲ့အပိုင်းတွေ ဖြစ်သွားပါပြီ။ ဒီအပိုင်းတွေကိုတော့ ထည့်သွင်းဖော်ပြနိုင်မှာ မဟုတ်ပါဘူး။

NiceHash လိုမျိုး အလားတူ နည်းပညာတွေ ရှိပါသေးတယ်။ စိတ်ဝင်စားလို့ လေ့လာကြည့်ချင်ရင် Cudo Miner နဲ့ Honey Miner တို့ကို လေ့လာကြည့်နိုင်ပါတယ်။

Cudo Miner – https://www.cudominer.com

Honey Miner – https://honeyminer.com

ဒီထက်အဆင့်မြင့်သွားရင်တော့ Mine တူးမယ့် ကွန်ပျူတာမှာ Mining Operating System တွေတင်သုံးလို့ ရနိုင်ပါသေးတယ်။ ဒါကတော့ နည်းပညာပိုင်း အတော်လေး နိုင်နင်းမှ ရမယ့်အဆင့် ဖြစ်သွားပါပြီ။ စိတ်ဝင်စားရင်တော့ NiceHash OS နဲ့ Hive OS တို့ကို လေ့လာနိုင်ပါတယ်။

NiceHash OS – https://www.nicehash.com/nhos-mining
Hive OS – https://hiveos.farm

Cryptocurrency Exchanges

Bitcoin နဲ့ပက်သက်ရင် နောက်ထပ် အမေးများတဲ့မေးခွန်းတွေ ကတော့ –

၁။ အဲ့ဒီ ကွိုင်တွေက ဘယ်မှာသုံးလို့ရလဲ။
၂။ ရိုးရိုးငွေနဲ့ရော ပြန်လဲပြီး ထုတ်လို့ရလား။

ဘယ်မှာသုံးလို့ရလဲဆိုတာကိုတော့ ခဏနေမှ ဆက်ပြောပါမယ်။ ဒုတိယမေးခွန်း အတွက် ကတော့ Cryptocurrency Exchanges တွေမှာ Bitcoin အပါအဝင် Cryptocurrency တွေကို ရိုးရိုးငွေအနေနဲ့ ပြန်ထုတ်ယူလို့ ရတယ်လို့ ဖြေရမှာပါ။ ဟိုးအရင် ယုံကြည်ရတဲ့ Exchange တွေ မပေါ်ခင်ကတော့ အင်တာနက် ဖိုရမ်တွေမှာ ချိန်းတွေ့ပြီး တိုက်ရိုက် အရောင်းအဝယ် လုပ်ကြရလို့ ငွေအလိမ်ခံရတဲ့ ဇာတ်လမ်းတွေလည်း အများကြီးဖြစ်ခဲ့ဖူးပါတယ်။ အခုတော့ ဒါမျိုးတွေမလိုအပ်တော့ပါဘူး။ ခိုင်မာတဲ့ Exchange တွေ ရှိနေပါပြီ။

Exchange ဆိုတာ တစ်ကယ်တော့ ဒေါ်လာငွေလဲ ကောင်တာလို ပုံစံမျိုးပါပဲ။ ဒါက ဘာကိုဆိုလိုတာလဲ မျက်စိလည်သွားမှာစိုးလို့ ပြောပြတာပါ။ ဒေါ်လာဝယ်ချင်ရင် ဘဏ် (သို့မဟုတ်) နီးစပ်ရာ ဒေါ်လာ လဲလို့ရတဲ့ Exchange ကောင်တာမှာ သွားဝယ်ယူလို့ရသလိုပါပဲ Cryptocurrency Exchange မှာ လိုချင်တဲ့ Cryptocurrency ကို သွားဝယ်ယူလို့ ရပါတယ်။ ကိုယ့်မှာ ဒေါ်လာရှိရင် ဒေါ်လာ Exchange ကောင်တာမှာ သွားရောင်းလို့ ရသလိုပဲ ကိုယ့် Cryptocurrency ကို Exchange မှာ သွားရောင်းလို့ ရတာပါ။

ဒီနေရာမှာ ဟိုးအစပိုင်းက ပြောခဲ့တဲ့ တရားဝင်မှု အခြေအနေကတော့ စကားပြောပါတယ်။ အမေရိကန် နိုင်ငံ နဲ့ ဥရောပလို တရားဝင်ခွင့်ပြုထားတဲ့ နိုင်ငံတွေမှာ အလွယ်တစ်ကူ ရရှိနိုင်ပြီး မြန်မာနိုင်ငံ အပါအဝင် တရားမဝင်ဘူးလို့ သတ်မှတ်ထားတဲ့ နိုင်ငံတွေမှာတော့ ခက်ပါလိမ့်မယ်။ ဒါက ရိုးရိုးငွေအနေနဲ့ လဲယူရ လွယ်ခြင်း မလွယ်ခြင်းနဲ့ မဆိုင်တော့ဘဲ၊ သက်ဆိုင်ရာနိုင်ငံမှာ Cryptocurrency တရားဝင်ခြင်း မဝင်ခြင်းနဲ့ သာ သက်ဆိုင်သွားပါတယ်။ လိုရင်းကတော့ <u>တရားဝင်တဲ့ နိုင်ငံတွေမှာ လဲရလွယ်ပြီး တရားမဝင်တဲ့ နိုင်ငံ တွေမှာတော့ ခက်ပါလိမ့်မယ်</u>။

လဲပုံလဲနည်းကတော့ Exchange တစ်ခုနဲ့တစ်ခု အသေးစိတ်လုပ်ငန်းစဉ်မှာ ကွာသွားနိုင်ပေမယ့် အခြေခံ အလုပ်လုပ်ပုံက ဒီလိုပါ။

၁။ သက်ဆိုင်ရာ Exchange မှာ အကောင့်ဖွင့်ရပါမယ်။ Exchange တွေ အများကြီးရှိပါတယ်။ ထင်ရှားပြီး လူသုံးများကြတဲ့ Exchange တွေကတော့ **Binance**, **Coinbase**, **KuCoin** နဲ့ **Kraken** တို့ဖြစ်ပါတယ်။ အဲ့ဒီ ထဲက Binance ဟာ အကြီးဆုံး Exchange ဖြစ်ပြီး တစ်နေ့တစ်နေ့ အရောင်းအဝယ် Daily Volume အနေ နဲ့ ဒေါ်လာ (၂၀) ဘီလီယံကနေ (၇၀) ဘီလီယံလောက်ထိ ရှိနေတဲ့ Exchange တစ်ခုပါ။ ရုံးချုပ်က မော်လ် တာမှာရှိပြီး စင်ကာပူမှာ အဓိကအခြေစိုက် အလုပ်လုပ်ပါတယ်။ Coinbase ကတော့ မကြာခင်မှာ IPO ဝင် တော့မယ့် အမေရိကန် ကုမ္ပဏီပါ။ နာမည်က Blockchain ရဲ့ Coinbase နဲ့ တူနေပါတယ်။ Coinbase လို့ ပြောလိုက်ရင် Blockchain Coinbase ကိုပြောတာလား၊ Coinbase Exchange ကိုပြောတာလား ဆိုတာကို သေချာပြောဖို့ လိုနိုင်ပါတယ်။ KuCoin ကလည်း စင်ကာပူအခြေစိုက် ကုမ္ပဏီဖြစ်ပြီးတော့ Kraken ကတော့ အမေရိကန် ကုမ္ပဏီတစ်ခုပါ။

Binance – https://www.binance.com

Coinbase – https://www.coinbase.com

KuCoin – https://www.kucoin.com

Kraken – https://www.kraken.com

အထက်မှာ ဝဘ်ဆိုက်လိပ်စာတွေကို ထည့်ပေးထားပါတယ်။ မိုဘိုင်း App တွေလည်း အသီးသီး ရှိကြလို့ သက်ဆိုင်ရာ App Store တို့ Play Store တို့မှာလည်း ရှာဖွေထည့်သွင်းလို့ရပါတယ်။

၂။ တချို့ Exchange တွေက အထောက်အထား ID ပြပြီး ကိုယ့်အကောင့်အတွက် KYC တင်ရပါတယ်။ KYC ဆိုတာ Know Your Customer ရဲ့အတိုကောက်ပါ။ ဒီက Kpay တို့ Wave Pay တို့အတွက် မှတ်ပုံတင်ပြပြီး အကောင့် Level မြှင့်ရသလိုပါပဲ။ တချို့ Exchange တွေကတော့ ဒါမျိုး မတောင်းပါဘူး။ သက်ဆိုင်ရာ Exchange အခြေစိုက်ရာ နိုင်ငံအစိုးရက KYC ယူရမယ်လို့ သတ်မှတ်ထားရင် Exchange က ယူရပါတယ်။

၃။ Mine တူးပြီး ရလို့ပဲဖြစ်ဖြစ်၊ တစ်ယောက်ယောက်က လွှဲပို့ထားလို့ပဲဖြစ်ဖြစ် ကိုယ်ဆီမှာ ရှိနေတဲ့ Bitcoin အပါအဝင် Cryptocurrency တွေကို Exchange မှာ Deposit လုပ်ပြီး ထည့်လိုက်လို့ပါတယ်။

၄။ ဒါမှမဟုတ် သတ်မှတ်ထားတဲ့ ငွေပေးချေစနစ် တစ်ခုခုကို အသုံးပြုပြီး Exchange ကနေ Bitcoin ကို ဝယ်ယူလို့လည်း ရနိုင်ပါတယ်။ လက်ခံတဲ့ ငွေပေးချေစနစ် အနေနဲ့ Credit Card, Debit Card, PayPal, ဘဏ်ငွေလွှဲ စသည်ဖြင့် Exchange နဲ့ အသုံးပြုသူရဲ့ နိုင်ငံပေါ် မူတည်ပြီး Option အမျိုးမျိုး ရှိနိုင်ပါတယ်။

၅။ Bitcoin ကို ရိုးရိုးငွေ ပြန်လဲလိုတဲ့အခါမှာလည်း အတူတူပါပဲ။ Credit Card အကောင့်ထဲကို တိုက်ရိုက် ထည့်ပြီး Withdraw လုပ်ယူလို့ ရသလို ဘဏ်ငွေလွှဲ စနစ်နဲ့လည်း Withdraw လုပ်ယူလို့ ရနိုင်ပါတယ်။ အသုံးပြုသူရဲ့ နိုင်ငံပေါ်မူတည်ပြီး ပေးထားတဲ့ Option တွေ ကွဲပြားသွားပါလိမ့်မယ်။

မြန်မာပြည်ကနေ အကောင့်ဆောက်လို့ ရမရ၊ မြန်မာပြည်မှာ အသုံးပြုနေကြတဲ့ Visa တို့ MasterCard တို့လို Credit Card, Debit Card တွေကို လက်ခံမခံ၊ မြန်မာပြည်ကို ဘဏ်တွေကို ငွေလွှဲလို့ ရမရ၊ ဒါတွေကိုတော့ ထည့်ပြောလို့မရပါဘူး။ အခုဒီလောက် ထည့်ပြောပြတယ်ဆိုတာလည်း ဗဟုသုတရအောင်သာ ဖော်ပြခြင်း ဖြစ်ပါတယ်။ ဒီစာရေးနေချိန်ထိ ဗဟိုဘဏ်ရဲ့ ထွက်ရှိထားတဲ့ ကြေညာချက်တွေအရ မြန်မာနိုင်ငံမှာ Cryptocurrency တွေကို အရောင်းအဝယ်၊ အလဲအလှယ် လုပ်တာဟာ တရားမဝင်ဘူး ဆိုတာကို ထပ်မံသတိပေးလိုပါတယ်။

Bitcoin ဘယ်မှာသုံးလို့ရလဲ

စောစောက ပြောလက်စဖြစ်တဲ့ မေးခွန်းတစ်ခုကို ပြန်ဆက်ပါမယ်။ Bitcoin ကို ဘယ်မှာ သုံးလို့ရလဲ။ လွန်ခဲ့တဲ့ နှစ်တချို့အတွင်း အဆပေါင်း (၁၀၀–၁၀၀၀) မက တန်ဖိုး တက်လာပြီး နောက်ကိုလည်း အဲ့ဒီလောက်မဟုတ်တောင်ရင်တောင် အတိုင်းအတာတစ်ခုထိ ဆက်တက်နေဦးမယ်လို့ ယူဆရတဲ့ Bitcoin ကို ရရှိပြီးနောက် သုံးပစ်မယ်ဆိုတာ တစ်ကယ်တော့ နှမြောစရာပါ။ ဒါပေမယ့် သုံးလို့ရမှ၊ အသုံးဝင်မှ တန်ဖိုးရှိမယ့်အရာတစ်ခုအနေနဲ့ ဘယ်မှာသုံးလို့ရလဲဆိုတာ မေးသင့်ပြီး လူတိုင်းသိချင်ကြမယ့် မေးခွန်းတစ်ခုပါ။

Apple က သူ့ရဲ့ Device တွေ ဝယ်ယူမှုအတွက် Bitcoin နဲ့ ငွေပေးချေတာကို လက်ခံခဲ့ဖူးပါတယ်။ ဒါပေမယ့် နောက်ပိုင်းမှာ ဈေးနှုန်းအတက်အကျ မြန်လွန်းပြီး များလွန်းတဲ့အတွက် လက်မခံတော့ပါဘူး လို့ ကြေညာပြီး အခုဒီစာရေးနေချိန်မှာတော့ လက်မခံတော့ပါဘူး။ ဒီစာရေးနေချိန်ဆိုတာကို ထည့်ပြောတာကို နောက်ပိုင်းမှာ Cryptocurrency တွေကို ပြန်လက်ခံလာမယ့် အလားအလာတွေ ရှိနေလို့ပါ။

Tesla ကလည်း သူ့ရဲ့ ကားတွေ ဝယ်ယူမှုအတွက် Bitcoin နဲ့ ငွေပေးချေတာကို အရင်က လက်ခံခဲ့ပါတယ်။ ကုမ္ပဏီအနေနဲ့လည်း (၁.၅) ဘီလီယံခန့် တန်ဖိုးရှိတဲ့ Bitcoin တွေ ဝယ်ယူ စုဆောင်းထားပါသေးတယ်။ ဒါပေမယ့် သိပ်မကြာခင်လေးကမှ Bitcoin Miner တွေရဲ့ လျှပ်စစ်စွမ်းအင် အလွန်အကျွံအသုံးပြုမှုကြောင့် ကာဗွန်ဒိုင်အောက်ဆိုဒ် ထုတ်လွှတ်မှုများတဲ့အတွက် လက်မခံတော့ဘူး လို့ ကြေညာခဲ့ပါတယ်။ ဒါကြောင့် Bitcoin ဈေးတွေထိုးကျသွားပြီး အခုဒီစာရေးနေချိန်ဟာ အဲ့ဒီလို Tesla ရဲ့ ကြေညာချက်ကို အကြောင်းပြုပြီး ဈေးတွေကျနေချိန် ဖြစ်ပါတယ်။

လျှပ်စစ်ကားကုမ္ပဏီတစ်ခုဖြစ်တဲ့ Tesla အတွက် သူ့ကားတွေဟာ ရေနံကထွက်တဲ့ လောင်စာဆီကို သုံးစရာမလိုလို့ တစ်ခြားကားတွေနဲ့ယှဉ်ရင် ကာဗွန်ဒိုင်အောက်ဆိုဒ် ထုတ်လွှတ်မှုမရှိဘူးဆိုတာ အဓိက အားသာချက်တစ်ခု ဖြစ်နေတာပါ။ သူ့အနေနဲ့ ဒီပုံရိပ်ကို ထိန်းသိမ်းဖို့ လိုအပ်တဲ့အတွက် ဒါကိုအကြောင်းပြုပြီး လက်မခံတော့တဲ့ သဘောမျိုးလို့ ဆိုနိုင်ပါတယ်။ ဒါပေမယ့် Bitcoin Mining ရဲ့ စွမ်းအင်အသုံးပြုမှု ၅၀% လောက်ကို တွင်းထွက်လောင်စာ မဟုတ်တဲ့ Renewable Energy အသုံးပြုနိုင်ပြီဆိုရင် ပြန်လက်ခံမယ် လို့လည်း Tesla ရဲ့ တည်ထောင်သူ Elon Musk က ထပ်ပြောထားပါသေးတယ်။ ဒါကြောင့် နောက်ပိုင်းမှာတော့ ပြန်လက်ခံဖို့ ရှိနေပါတယ်။

Apple တို့ Tesla တို့ဆိုတာ အလွန်အရေးပါတဲ့ လုပ်ငန်းကြီးတွေမို့လို့ သူတို့အကြောင်း အရင်ပြောတာပါ။ လက်တွေ့အသုံးပြုမှုနဲ့ ပက်သက်ရင် Binance လို Exchange မျိုးက Cryptocurrency တွေအတွက် Binance Visa Card ကို ထုတ်ပေးပါတယ်။ ဒါကြောင့် Visa Card သုံးလို့ရတဲ့ နေရာတွေမှာ အသုံးပြုလို့ ရသွားပြီမို့လို့ ဘယ်နေရာမှာရတယ်ဆိုတာ ခေါင်းစဉ်တပ်ပြောဖို့ မလိုတော့ပါဘူး။ အသုံးပြုတာက တစ်ကမ္ဘာလုံး ကြိုက်တဲ့နေရာမှာ သုံးလို့ရပေမယ့် ကဒ်ထုတ်ပေးတာကိုတော့ လောလောဆယ် ဥရောပ နိုင်ငံတွေအတွက်ပဲ ပေးပါသေးတယ်။

https://www.binance.com/en/cards

Coinbase ကလည်း လာမယ့်လအချို့အတွင်းမှာ Coinbase Card ကို ထုတ်ပေးဖို့ ရှိပါတယ်။ အဲ့ဒီလိုပဲ Coinbase Exchange က Visa နဲ့ပေါင်းပြီး ထုတ်ပေးတာပါ။ သူလည်း တစ်ကမ္ဘာလုံး Visa လက်ခံတဲ့ နေရာတိုင်းမှာ အသုံးပြုလို့ရပါတယ်။ ကဒ်ထုတ်ပေးတာကတော့ နိုင်ငံအကန့်အသတ် ရှိပါလိမ့်မယ်။

https://www.coinbase.com/card

ဒါကြောင့် Bitcoin ကို ဘယ်မှာသုံးလို့ရမလဲဆိုရင် ဒီလိုကဒ်တွေ ရတဲ့သူအတွက်ကတော့ နေရာတိုင်းလိုလိုမှာ သုံးလို့ရနေပြီလို့ ဆိုရမှာပါ။ Visa လက်မခံတဲ့ ဆိုင်တွေ၊ နေရာတွေ ရှိပေမယ့် လိုအပ်ရင် Visa ကဒ် လက်ခံတဲ့ ATM ကနေလည်း ငွေသား Cash ထုတ်ယူလို့ ရနိုင်ပါသေးတယ်။

ဒါကနည်းနည်းတော့ ပြောင်းပြန်ဖြစ်ကောင်း ဖြစ်နေပါလိမ့်မယ်။ ဘဏ်တွေရဲ့ ဗဟိုထိန်းချုပ်မှုကို မလိုလား လို့ ထွက်ပေါ်လာတဲ့ Cryptocurrency အတွက် Binance တို့ Coinbase တို့က ဘဏ်ကဲ့သို့ ဗဟိုထိန်းချုပ်မှု ကို ပြန်ကိုင်လိုက်သလို ဖြစ်နေပါတယ်။ ဒီလို Exchange တွေကနေတစ်ဆင့် မဟုတ်ဘဲ တိုက်ရိုက် အပေးအယူလုပ်ချင်တယ်ဆိုရင်လည်း သုံးလို့ရတဲ့ နေရာတွေ အများအပြား ရှိပါတယ်။

Game တို့ VPN တို့ Domain Name တို့လို ဒစ်ဂျစ်တယ်ထုတ်ကုန်တွေကတော့ Bitcoin နဲ့ အချိန်မရွေး ဝယ်ယူလို့ ရနိုင်ပါတယ်။ Wikipedia ကို လှူချင်ရင်လည်း Bitcoin နဲ့လှူလို့ရပါတယ်။ ဒီလို ဒစ်ဂျစ်တယ် ထုတ်ကုန်နဲ့ အလှူအတန်း တင်မကပါဘူး တစ်ကယ့် ရွှေအစစ်နဲ့ ငွေအစစ်တွေ ဝယ်ချင်ရင် **Bitgild** လို နေရာမျိုးမှာ Bitcoin နဲ့ ဝယ်လို့ရပါတယ်။ Tesla က Bitcoin ကို လက်မခံတော့ဘူး ဆိုပေမယ့် Tesla အပါအဝင် ကားအမျိုးမျိုးကို **BitCars** မှာ Bitcoin နဲ့ ဝယ်လို့ရပါတယ်။ အိမ်ဝယ်ချင်ရင်လည်း **BitHome** မှာ ဝယ်လို့ရပါသေးတယ်။ ဖုန်း၊ ကွန်ပျူတာနဲ့ Device တွေ ဝယ်ချင်ရင်တော့ **Newegg** လို့ခေါ်တဲ့ ထင်ရှား တဲ့ e-Commerce ပလက်ဖောင်းက Bitcoin နဲ့ လက်ခံပေးပါတယ်။ ခရီးတွေဘာတွေ ထွက်ချင်လို့ ဟော်တယ်ခကို Bitcoin နဲ့ပေးပြီး လေယာဉ်လက်မှတ်ကို Bitcoin နဲ့ဝယ်ချင်ရင်လည်း ရပါတယ်။ **Travala** မှာ တစ်ကမ္ဘာလုံးလိုလိုအတွက် ခရီးစဉ်တွေ Booking လုပ်လို့ရပြီး Bitcoin နဲ့လက်ခံပါတယ်။

Bitgild – https://www.bitgild.com

BitCars – https://bitcars.eu

BitHome – https://bithome.ch

Newegg – https://www.newegg.com

Travala – https://www.travala.com

ဒါတွေမြန်မာပြည်မှာ ရတာလားလို့တော့ မမေးနဲ့ပေါ့။ လက်တွေ့ကမ္ဘာမှာ ဒီလိုတွေ အသုံးပြုလို့ ရနေတယ် ဆိုတာကို မြင်သာစေဖို့အတွက်သာ ထည့်ပြောပြတာပါ။

ဝေဖန်ချက်နှင့် ကန့်သတ်ချက်များ

Bitcoin နဲ့ပက်သက်ရင် ထောက်ခံအားပေးသူတွေ ရှိကြသလို၊ ဝေဖန်ဆန့်ကျင်သူတွေလည်း ရှိကြပါတယ်။ ကမ္ဘာ့အချမ်းသာဆုံး သူဌေးကြီးတွေထဲမှာ ပါဝင်တဲ့ Warren Buffet ရဲ့ ဝေဖန်ချက်နဲ့ Bill Gates ရဲ့ ဝေဖန်ချက်တို့ဟာ Bitcoin နဲ့ပက်သက်ရင် အဓိကအကျဆုံးနဲ့ မကြာမကြာ တွေ့ရတဲ့ ဝေဖန်ချက်တွေပါ။

Warren Buffet က Bitcoin ဟာ တန်ဖိုးအစစ်အမှန် မရှိတဲ့ အရာတစ်ခု လို့ ဝေဖန်ထားပါတယ်။ တန်ဖိုးအစစ်အမှန်ဆိုတာ သူကိုယ်တိုင်မှာ ကုန်ထုတ်စွမ်းအား မရှိသလို ကုန်ထုတ်စွမ်းအားတိုးတက်စေဖို့ အားပေးတဲ့ ဂုဏ်သတ္တိလည်း မရှိဘူးဆိုတဲ့သဘောပါ။ နောက်လူက ဈေးပိုပေးရင် မြတ်မယ်၊ မပေးရင် ရှုံးမယ်ဆိုတဲ့ ကြိုက်ရောင်းကြိုက်ဝယ် သဘောသက်သက်ပဲ ရှိတယ်လို့ ဆိုပါတယ်။

Bill Gates ကတော့ လူ့သမိုင်းတစ်လျှောက် ရှိရှိခဲ့ဖူးသမျှ ငွေပေးငွေယူစနစ်တွေထဲမှာ Bitcoin က လျှပ်စစ်စွမ်းအင်သုံးစွဲမှုအမြင့်ဆုံးပဲ လို့ဆိုပါတယ်။

တစ်ခြား ဝေဖန်သူအများ အဓိကပြောကြတာလည်း ဒီ (၂) ချက်ပါပဲ။ Bitcoin မှာ တန်ဖိုးအစစ်အမှန်မရှိဘူးဆိုတဲ့ အချက်နဲ့ Bitcoin ရဲ့ လျှပ်စစ်စွမ်းအင် သုံးစွဲမှုက လက်ခံနိုင်စရာမရှိဘူးဆိုတဲ့ အချက်တွေပါ။ ဒါတွေနဲ့ပက်သက်တဲ့ ဖြေရှင်းချက်တွေလည်း ရှိနေပါတယ်။ တန်ဖိုးအစစ်အမှန်ဆိုတာ တစ်နေရာရာကနေ ဆင်းသက်တာမဟုတ်ဘူး။ လူတွေကသတ်မှတ်ထားတာပါ။ အသုံးဝင်တဲ့အရာတစ်ခုကို လူတွေလိုချင်ရင် လူတွေသတ်မှတ်တဲ့ တန်ဖိုးတစ်ခု အဲ့ဒီအရာမှာ ရှိသွားတယ်လို့ ဆိုကြပါတယ်။ ဒီသဘောကို ရှေ့ပိုင်းမှာလည်း ထည့်ပြောထားခဲ့ပါတယ်။ ဥပမာ – ဇင်ဘာဘွေနိုင်ငံရဲ့ ငွေစက္ကူကို သူ့အစိုးရက တန်ဖိုးတွေ ဘယ်လိုပဲ သတ်မှတ်ထားပါစေ ပြည်သူတွေက အဖိုးတန်တယ်လို့ လက်မခံတော့တဲ့အခါ စက္ကူစုတ်လောက်တောင် တန်ဖိုးမရှိတော့ဘူး ဖြစ်သွားတာမျိုးပါ။

Bitcoin ဟာ လုံခြုံစိတ်ချစွာ သိမ်းဆည်းနိုင်ပြီး၊ ကြားခံမလိုဘဲ တိုက်ရိုက်ဖလှယ်နိုင်ခြင်းဆိုတဲ့ ဂုဏ်သတ္တိတွေ ရှိနေပါတယ်။ ဒီဂုဏ်သတ္တိကို လူတွေကလိုလားပြီး တန်ဖိုးထားကြတဲ့အခါ တန်ဖိုးရှိသွားတယ်၊ ဒီတန်ဖိုးဟာ စစ်မှန်တယ်လို့ ဖြေရှင်းကြပါတယ်။ ဒါဟာလက်ရှိအငြင်းပွားနေတဲ့ ကိစ္စမို့လို့ စာရေးသူကတော့ အချက်အလက်ကိုသာ တင်ပြပါတယ်။ ဝေဖန်ချက်ကို လက်ခံခြင်း၊ လက်မခံခြင်းနဲ့ ဖြေရှင်းချက်ကို လက်ခံခြင်း၊ လက်မခံခြင်းကတော့ စာဖတ်သူကပဲ ကိုယ်တိုင်ဆုံးဖြတ်ရမှာပါ။

ဒုတိယအဓိကဝေဖန်ချက်ဖြစ်တဲ့ လျှပ်စစ်စွမ်းအင်သုံးစွဲမှုကတော့ လက်ရှိ Bitcoin Miner တွေ အသုံးပြုနေကြတဲ့ နှစ်စဉ်စွမ်းအင်ဟာ ခန့်မှန်းခြေ 110 Terawatt Hours per Year ရှိတယ်လို့ဆိုပါတယ်။ ဒါဟာ နယ်သာလန်နိုင်ငံရဲ့ တစ်နှစ်တာစွမ်းအင်အသုံးပြုမှုနီးပါးရှိပြီး ဘယ်လ်ဂျီယန်၊ ဖင်လန်၊ ဆွစ်ဇာလန် တို့လို နိုင်ငံတွေရဲ့ တစ်နှစ်တာ စွမ်းအင်အသုံးပြုမှုထက်ကိုတောင် ကျော်လွန်နေတဲ့ ပမာဏပါ။ မြန်မာနိုင်ငံအတွက်ဆိုရင် လက်ရှိ မြန်မာနိုင်ငံမှာ အသုံးပြုနေတာက 18 Terawatt Hours per Year ဆိုတော့ <u>Bitcoin တစ်နှစ် Mine တဲ့ စွမ်းအင်ကို မြန်မာနိုင်ငံ တစ်နိုင်ငံလုံး (၆) နှစ်စာလောက် အသုံးပြုလို့ ရနိုင်တယ်</u> လို့ဆိုရပါမယ်။

နိုင်ငံတွေရဲ့ စွမ်းအင်အသုံးပြုမှုကို ဒီ Wikipedia Article ကနေ ကိုးကားထားပါတယ်။

https://en.wikipedia.org/wiki/List_of_countries_by_electricity_consumption

တန်ဖိုးမရှိတဲ့အရာတစ်ခုအတွက် နိုင်ငံတစ်ခုစာ လျှပ်စစ်စွမ်းအင်ကို သုံးနေတာဟာ အကျိုးမဲ့ဖြုန်းတီးခြင်းဖြစ်တယ်လို့ ဝေဖန်ကြတာပါ။ အထူးသဖြင့် ကနေ့ခေတ်လို Global Warming ခေါ် ကမ္ဘာကြီးပူနွေးလာမှုဟာ လူသားထု တစ်ရပ်လုံးအတွက် အန္တရာယ်လို့ သဘောထားနေကြချိန်မှာ ဒါမျိုး အသုံးပြုနေတော့ ပိုဆိုးပါတယ်။ သုတေသနစာတမ်းတစ်စောင်က Bitcoin ကြောင့် ကမ္ဘာကြီး ၂ ဒီဂရီစင်တီဂရိတ်ထိ ပိုပြီးပူနွေးလာနိုင်တယ်လို့ ဖော်ပြထားပြီး ဒီစာတမ်းကိုလည်း ကိုးကားဝေဖန်ကြတာပါ။

https://www.nature.com/articles/s41558-018-0321-8

ဒီဝေဖန်ချက်နဲ့ပက်သက်ပြီး တုံ့ပြန်ချက်ကတော့ အခြားသောငွေပေးငွေယူ စနစ်တွေလည်ပါတ်ဖို့အတွက် ဗဟိုဘဏ်၊ ဘဏ် နဲ့ Payment Processor တို့ ပူးပေါင်းအလုပ်လုပ်ကြရပါတယ်။ တစ်ကမ္ဘာလုံး အတိုင်းအတာနဲ့ ဒီအဖွဲ့အစည်းတွေ လည်ပါတ်ဖို့အတွက် အသုံးပြုနေကြတဲ့ လျှပ်စစ်စွမ်းအင်ဟာ Bitcoin Network က အသုံးပြုနေတဲ့ လျှပ်စစ်စွမ်းအင်ထက် အများကြီးပိုပါတယ်လို့ တုံ့ပြန်ကြပါတယ်။

ပြီးတော့ Bitcoin Miner တွေဟာ တွင်းထွက် လောင်စာကိုချည်းပဲ အသုံးပြုနေတာ မဟုတ်ပါဘူး။ တရုတ်နိုင်ငံမှာ အဓိက Mining Firm ကြီးတွေ ရှိပြီး တချို့ Firm တွေက ကျောက်မီးသွေးလို တွင်းထွက်လောင်စာက ရတဲ့လျှပ်စစ် စွမ်းအင်ကို သုံးနေပေမယ့်၊ တချို့ Firm တွေကတော့ ရေအားလျှပ်စစ် ကရတဲ့ Renewable Energy ကိုအသုံးပြုနေကြပါတယ်။ Renewable Energy ကနေ ရတဲ့ လျှပ်စစ်စွမ်းအင်က

ဈေးနှုန်း ပိုချိုသာလို့ Mine တူးတဲ့သူတွေအတွက်လည်း ပိုကိုက်ပါတယ်။ ဒါကြောင့် အခုကတည်းက Bitcoin Mining ရဲ့ ရာခိုင်နှုန်းတချို့ဟာ Renewable Energy ကို အသုံးပြုနေကြပြီး၊ Renewable Energy တီထွင်မှု ပိုင်းကို အရင်ထက် ပိုမြန်သွားအောင် တွန်းအားပေးနေပါသေးတယ်လို့လည်း တုံ့ပြန်ကြပါတယ်။

ထုံးစံအတိုင်း ဝေဖန်ချက်နဲ့ တုံ့ပြန်ချက်တွေပေါ်မှာ စာဖတ်သူကိုယ်တိုင်ပဲ ချင့်ချိန်ဆုံးဖြတ်ရမှာပါ။ ဒီနှစ်ချက်က အဓိက ဆိုပေမယ့် လုံခြုံမှုနဲ့ပက်သက်တဲ့ ဝေဖန်ချက်တွေ ဈေးနှုန်းအတက်အကျ ကြမ်းခြင်းနဲ့ ပက်သက်တဲ့ ဝေဖန်ချက်တွေလည်း ရှိတော့ရှိပါသေးတယ်။

လုံခြုံမှုနဲ့ပက်သက်တဲ့ ဝေဖန်ချက်တွေကတော့ Blockchain ရဲ့သဘောသဘာဝကို လူတွေပိုနားလည်လာကြခြင်းနဲ့အမျှ သိပ်မပြောကြတော့ပါဘူး။ ဈေးနှုန်းအတက်အကျ ကြမ်းတာကတော့ အမှန်ပါ။ တစ်ခြား ဒေါ်လာတို့ ရွှေတို့ အိမ်ခြံမြေတို့လို ရင်းနှီးမြှုပ်နှံမှုတွေနဲ့ နှိုင်းယှဉ်လို့ မရအောင် အတက်အကျ ကြမ်းပါတယ်။ ဒေါ်လာဈေး 5% ကျသွားရင်သာ ပြဿနာခတ်ကြရပေမယ့် Bitcoin မှာ ဈေးနှုန်း 5% လောက် တက်သွားတယ်၊ ကျသွားတယ်ဆိုတာ မိနစ်ပိုင်းအတွင်း အမြဲ ဖြစ်နေတာပါ။ တစ်ခြား ရင်းနှီးမြှုပ်နှံမှုတွေမှာ 10% လောက်မြတ်ရင် အတော်ဟုတ်နေပါပြီ။ Bitcoin နဲ့ Cryptocurrency မှာ ရင်းနှီးမြှုပ်နှံကြသူတွေက 100% အမြတ်လောက်ကို အနိမ့်ဆုံးမှန်းထားကြတာပါ။ 10x တို့ 100x တို့လို အရှုံးအမြတ်မျိုးနဲ့ ဆယ်ဆ၊ အဆတစ်ရာ အရှုံးအမြတ်ဆိုတာ Cryptocurrency မဖြစ်နိုင်တဲ့အရာတွေ မဟုတ်ပါဘူး။ အဲ့ဒီလောက်ထိ အတက်အကျ ကြမ်းပါတယ်။ ဒါပေမယ့် အခုနောက်ပိုင်းမှာတော့ ဈေးကွက်တည်ငြိမ်လာခြင်းနဲ့အတူ ဟိုအရင်ကလောက်ထိတော့ အတက်အကျမကြမ်းတော့ပါဘူး။ ကြမ်းတော့ကြမ်းပါသေးတယ်။ ဒါပေမယ့် အရင်ထက်စာရင်တော့ အများကြီးပိုငြိမ်နေပါပြီ။

တစ်ကယ့်တော့ Bitcoin ရဲ့ ပြဿနာက အဲ့ဒါတွေ မဟုတ်သေးပါဘူး။ Bitcoin ရဲ့အဓိကပြဿနာက အခုမှလာမှာပါ။

Bitcoin ဟာ (၁၀) မိနစ်မှာတစ်ကြိမ်သာ Blockchain ထဲကို Block အသစ်ထည့်ရတဲ့ နည်းပညာဖြစ်ပြီး Block တစ်ခုမှာ Transaction (၄၀၀၀) ခန့်သာပါဝင်နိုင်လို့၊ (၁၀) မိနစ်မှာ Transaction (၄၀၀၀) သာ ပြုလုပ်နိုင်တယ်ဆိုတဲ့ အဓိပ္ပါယ်ပါ။ တစ်နည်းအားဖြင့် အမြင့်ဆုံး 6.5 Transaction per Second ခန့်ပဲရှိပါတယ်။ တစ်စက္ကန့်မှာ Transaction (၆.၅) ခုလောက်ထိပဲ လုပ်ပေးနိုင်ပါတယ်။

နိုင်းယှဉ်ကြည့်မယ်ဆိုရင် လက်ရှိ အကြီးဆုံး Payment Processor ဖြစ်တဲ့ Visa ဟာ လက်ရှိ 2,000 Transaction per Second ဝန်းကျင်မှာ အလုပ်လုပ်နေပါတယ်။ လိုအပ်ရင် 65,000 Transaction per Second ထိ လုပ်ပေးနိုင်တယ်လို့လည်း ဆိုထားပါတယ်။ ဒါကြောင့် တစ်ကမ္ဘာလုံးက အသုံးပြုနိုင်တဲ့ ငွေပေးငွေယူစနစ်ဖြစ်ဖို့ဆိုရင် အနည်းဆုံးအနေနဲ့ 2,000 Transaction per Second အလုပ်လုပ်ပေးနိုင်ဖို့ လိုအပ်ပါတယ်။ Bitcoin ကတော့ 6.5 Transaction per Second လောက်သာ အလုပ်လုပ်ပေးနိုင်လို့ သူ့ချည်းသက်သက်နဲ့ တစ်ကမ္ဘာလုံး အသုံးပြုနိုင်တဲ့ ငွေပေးငွေယူစနစ် ဖြစ်လာနိုင်မှာ မဟုတ်ပါဘူး။

ဒီပြဿနာကို ဖြေရှင်းဖို့အတွက် Lightning Network လို ထပ်တိုးနည်းပညာသစ်တွေနဲ့ Layer-2 Scalability Solution တွေ ထွက်ပေါ်နေပြီ ဖြစ်ပေမယ့် ဒီအကြောင်းတွေကို မပြောနိုင်သေးပါဘူး။ လောလောဆယ် Bitcoin မှာ Scalability Issue ခေါ် အများသုံးအဆင့် ဖြစ်လာဖို့အတွက် အဟန့်အတား ပြဿနာတစ်ခု အမှန်တစ်ကယ် ရှိနေတယ်လို့ မှတ်သားရမှာပါ။

နောက်ထပ် အရေးကြီးတဲ့ Bitcoin ရဲ့ ပြဿနာကတော့ Max Supply အဖြစ် ကွိုင် (၂၁) သန်းမှာ ကန့်သတ်ထားခြင်းပဲဖြစ်ပါတယ်။ ဒီလိုကန့်သတ်ထားတဲ့အတွက် ရှားပါးပြီး အဖိုးတန်သွားပေမယ့် ဒီလို အဖိုးတန်သွားတဲ့ အတွက်ကြောင့်ပဲ ထုတ်မသုံးဘဲ စုထားတဲ့သူတွေ ပိုများနေနိုင်ပါတယ်။ ရ ထားတဲ့ Bitcoin တွေကို သုံးပစ်ရမှာ နမြောစရာကြီးလို့ အထက်မှာ ပြောခဲ့ပါသေးတယ်။ ဒီလိုစုထားကြရင်တော့ ငွေလည်ပါတ်မှုနှုန်း Circulation ကျပြီး လူတိုင်းသုံးတဲ့ ငွေပေးငွေယူစနစ် ဖြစ်လာနိုင်မှာ မဟုတ်ပါဘူး။

ဒါကြောင့်လည်း အခုနောက်ပိုင်းမှာ Bitcoin ကို Currency လို့ သဘောမထားကြတော့ပါဘူး။ ဒါအလွန် အရေးကြီးပါတယ်။ အခုနောက်ပိုင်းမှာ <u>Bitcoin ကို Store of Value လို့ပဲ သဘောထားကြပါတယ်</u>။ ရွှေကဲ့သို့ အဖိုးတန်သောအရာလို့ သဘောထားပါတယ်။ Digital Gold လို့ သဘောထားကြပါတယ်။ လုံခြုံစိတ်ချစွာ ကိုယ်တိုင် သိုလှောင် လွှဲပြောင်းနိုင်သော အဖိုးတန်အရာတစ်ခုပေါ့။ အသုံးပြုကြတဲ့အခါ Bitcoin ကို ငွေစက္ကူလို သဘောထားပြီး အသုံးပြုရမှာ မဟုတ်ဘဲ ရွှေလို သဘောထားပြီး အသုံးပြုကြရမှာပါ။

Currency အနေနဲ့ အသုံးပြုဖို့အတွက်ဆိုရင် Bitcoin ထက်ပိုပြီးသင့်တော်တဲ့ အခြား Cryptocurrency တွေရှိနေပါတယ်။ ဒီအကြောင်းကိုတော့ ခဏနေမှ ဆက်ပြောပါမယ်။

အခန်း (၅) – စိတ်ဝင်စားဖွယ်ဖြစ်ရပ်များနှင့် လိမ်လည်မှုများ

Bitcoin Pizza Day

မေလ (၂၂) ရက်နေ့ကို Bitcoin Pizza Day လို့ သတ်မှတ်ထားကြပါတယ်။ ဘာဖြစ်လို့လဲဆိုတော့ အဲ့ဒီနေ့မှာ သမိုင်းဝင်ဖြစ်ရပ်တစ်ခု ဖြစ်ပွားခဲ့လို့ပါ။ ၂၀၁၀ ခုနှစ်၊ မေလ (၁၇) ရက်နေ့မှာ အမေရိကန်နိုင်ငံ ဖလော်ရီဒါမှာ နေထိုင်သူ Laszlo Hanyecz ဆိုသူတစ်ဦးက သူ့ကို ပီဇာနှစ်ချပ်လောက် လာပို့ပေးရင် Bitcoin (၁၀,၀၀၀) ပေးမယ်လို့ ကြေညာခဲ့ပါတယ်။

အဲ့ဒီအချိန်မှာ (၁၉) နှစ်အရွယ်သာ ရှိသေးတဲ့ ကျောင်းသားတစ်ဦးဖြစ်သူ Jeremy Sturdivant ဆိုသူက ပီဇာနှစ်ချပ်ကို အမှန်တစ်ကယ် လာပို့ပေးခဲ့တဲ့အတွက် မေလ (၂၂) နေ့မှာ Laszlo က Jeremy ကို Bitcoin (၁၀,၀၀၀) ပေးချေခဲ့ပါတယ်။ ဒါဟာ Bitcoin ကို အသုံးပြုပြီး ပထမဆုံးအကြိမ် ငွေပေးငွေယူလုပ်ခဲ့တဲ့ မှတ်တမ်း ဖြစ်သွားပါတော့တယ်။

အဲ့ဒီအချိန်က Bitcoin (၁၀,၀၀၀) ရဲ့ တန်ကြေးဟာ $41 ခန့်သာ ရှိခဲ့တာပါ။ အခုဒီစာရေးနေချိန် ပေါက်ဈေးနဲ့သာဆိုရင်တော့ ဒေါ်လာ သန်း (၃၄၀) ကျော် တန်နေတဲ့ပမာဏပါ။ ဒါဟာ တွေးကြည့်မယ်ဆိုရင် ရယ်ရခက်၊ ငိုရခက် ဆိုတဲ့အခြေအနေတစ်ရပ်ပါ။ ပီဇာနှစ်ချပ် စားရဖို့အတွက် ဒေါ်လာသန်းပေါင်းများစွာ တန်မယ့်အရာကို ပေးလိုက်ရတာကိုး။ ဒါပေမယ့် နောက်ပိုင်းမှာ မေးမြန်းကြည့်တဲ့အခါ Laszlo က သူရဲ့လုပ်ရပ်အတွက် လုံးဝနောင်တရ ဝမ်းနည်းနေခြင်း မရှိဘူးလို့ ဆိုပါတယ်။ ဒီလို အပြောင်းအလဲတစ်ခုရဲ့ သမိုင်းမှတ်တမ်းအနေနဲ့ ဝင်သွားတာကိုပဲ သူကကျေနပ်နေတာပါ။

Bitcoin (၁၀,၀၀၀) တန် ပီဇာနှစ်ချပ်နှင့် Laszlo Hanyecz တို့မိသားစု

Bitcoin (၁၀,၀၀၀) ကိုလက်ခံရရှိတဲ့ Jeremy ကရော အခု သန်းကြွယ်သူဌေးကြီး ဖြစ်နေပြီလား။ သန်းကြွယ်သူဌေး ဖြစ်မဖြစ်တော့ မသိပါဘူး။ သူကလည်း အဲ့ဒီ Bitcoin (၁၀,၀၀၀) ရဲ့တန်ကြေး $400 ဖြစ်သွားချိန်မှာ အကုန်သုံးလိုက်ပြီလို့ ဆိုပါတယ်။ သူကလည်း အင်တာဗျူးတစ်ခုမှာ အခုလို နောက်ထားပါသေးတယ် – “Give a man a pizza, he'll eat for a day, let him buy pizza with bitcoin, revolutionize the economy.” တဲ့။ နောင်တရ ဝမ်းနည်းနေတဲ့ပုံတော့ မဟုတ်ပါဘူး။

ဒီဖြစ်ရပ်ကို ဂုဏ်ပြုတဲ့အနေနဲ့ အခုဆိုရင် မေလ (၂၂) ရက်နေ့ကို Bitcoin Pizza Day လို့သတ်မှတ်ပြီး အဲ့ဒီနေ့ရောက်တိုင်း ကမ္ဘာအနှံ့အပြားက Cryptocurrency နဲ့ပက်သက်ပြီး တက်ကြွသူတွေဟာ ပီဇာစားပြီး အောင်ပွဲခံကြပါတယ်။

ကွိုင်ပျောက်ကြသူများ

Stefan Thomas လို့ခေါ်တဲ့ ဆန်ဖရမ်စစ္စကိုမှာ နေထိုင်သူတစ်ဦးရဲ့ အဖြစ်ကတော့ New York Times ကတောင် သတင်းဆောင်းပါးလုပ် ရေးခဲ့ရပါတယ်။ Bitcoin ပေါင်း (၇,၀၀၂) ကွိုင် ရှိတဲ့ Wallet ကို ထည့်သိမ်းထားမိတဲ့ USB Stick ကို ဖွင့်ဖို့အတွက် ပတ်စ်ဝပ် မေ့နေတာပါ။ ကနေ့ပေါက်ဈေးနဲ့ဆိုရင် ဒေါ်လာသန်း (၂၀၀) ကျော်ဖိုး ရှိပါတယ်။ သူက Laszlo လို ဈေးပေါချိန်မှာ သူများကို ပေးလိုက်မိတာမဟုတ်ပါဘူး။ ဈေးတွေတက်နေချိန်မှာ လက်ထဲရှိနေပြီး ဖွင့်မရတာပါ။ ပိုဆိုးပါတယ်။

ဖြစ်ချင်တော့ အဲ့ဒီ USB Stick ကလည်း နှယ်နှယ်ရရ မဟုတ်ဘဲ IronKey လို့ခေါ်တဲ့ လုပ်ငန်းသုံးအဆင့် လုံခြုံရေးပစ္စည်းဖြစ်နေပါတယ်။ သတ်မှတ်အကြိမ် အရေအတွက်ထက် ပိုပြီး ပတ်စ်ဝပ် မှားလို့ မရပါဘူး။ သတ်မှတ်အကြိမ်ရေထက် ပိုမှားခဲ့ရင် အထဲက ဒေတာတွေကို အလိုအလျှောက် ဖျက်ပစ်လိုက်မှာပါ။ ပိုင်ရှင်ရဲ့ လုံခြုံရေးအတွက် အခိုးခံရတဲ့အခါ ခိုးယူသူက အထဲကအချက်အလက်တွေကို ယူလို့မရအောင် စီမံထားတာ ဖြစ်ပါတယ်။ (၁၀) ကြိမ်ပဲ မှားလို့ ရပါတယ်။ (၈) ကြိမ် စမ်းကြည့်ပြီးပါပြီ။ အဆင်မပြေပါဘူး။ နောက်ထပ် (၂) ကြိမ်ပဲ မှားခွင့်ကျန်တော့လို့ သူ့မှာ ထပ်မစမ်းရဲတော့ဘဲ ဒုက္ခရောက်နေချိန်မှာ ရေးခဲ့တဲ့ သတင်းဆောင်းပါး ဖြစ်ပါတယ်။

https://www.nytimes.com/2021/01/12/technology/bitcoin-passwords-wallets-fortunes.html

တစ်ကယ်တော့ အဲ့ဒီလို ပျောက်ဆုံးသွားတဲ့ ကွိုင်တွေမှ အများကြီးရှိပါတယ်။

James Howells လို့ခေါ်တဲ့ ဗြိတိန်နိုင်ငံက လူတစ်ယောက်ဆိုရင်လည်း အဲ့ဒီလိုပဲ၊ Bitcoin (၇,၅၀၀) ကျော် သိမ်းထားတဲ့ Hard Drive အဟောင်းတစ်လုံးကို ပစ္စည်းတွေရှင်းရင်း မှားပြီး အမှိုက်ပုံးထဲ လွှင့်ပစ်ခဲ့မိတယ်။ သတိရတဲ့အချိန်မှာ အမှိုက်သိမ်းကားက လာသိမ်းပြီး ပစ်လိုက်ပြီဖြစ်လို့ စည်ပင်အမှိုက်ပုံကြီးထဲကို ရောက်နေပါပြီ။ အဲ့ဒီ Hard Drive ကို အမှိုက်ပုံထဲကနေ ပြန်ရှာဖို့ မြို့နယ်ကောင်စီနဲ့ ညှိပါသေးတယ်။ ပေါင်သန်း (၂၀၀) လောက် တန်ကြေးရှိလို့ ပေါင်သန်း (၅၀) ကို ကောင်စီကို ပေးပါ့မယ်လို့ ညှိပေမယ့် ကောင်စီက သဘောမတူလို့ ပြန်ရှာခွင့် မရလိုက်ဘူး။ အမှိုက်ပုံကြီးကို ရှင်းပြီးရှာဖို့ ပေါင်သန်းချီ ကုန်မှာဖြစ်ပြီး အဲ့ဒီလို ရှာရင်တောင် ပြန်တွေ့ဖို့ မသေချာတဲ့အတွက်ကြောင့်ပါ။

https://www.theguardian.com/uk-news/2021/jan/14/man-newport-council-50m-helps-find-bitcoins-landfill-james-howells

ဒီဖြစ်ရပ်တွေက သတင်းထဲပါလာလို့ သိကြရပေမယ့် သတင်းထဲမပါဘဲ ပျောက်ဆုံးသွားတဲ့ Bitcoin တွေမှ အများကြီးရှိနေပါတယ်။ ခန့်မှန်းခြေအားဖြင့် ပျောက်ဆုံးသွားတဲ့ Bitcoin ပေါင်း (၂) သန်းလောက်ရှိတယ်လို့ သိရပါတယ်။ Bitcoin တီထွင်ခါစက Mine လုပ်တဲ့သူ နည်းနည်းပဲ ရှိပြီးတော့ တန်ဖိုးလည်း သိပ်မရှိလို့ ဒီလောက် အလေးမထားခဲ့ကြပါဘူး။ ခပ်ပေါ့ပေါ့ပဲ ထားလိုက်လို့ ပျောက်သွားပြီး အခုလိုဈေးတွေ အရမ်းတက်နေတော့မှပဲ နောင်တရကြတာပါ။

ဒီလိုမျိုးပြန်မရနိုင်တော့ဘဲ ဆုံးရှုံးသွားတဲ့ ကွိုင်တွေကို **Deadcoin** လို့ခေါ်ကြပါတယ်။ Bitcoin ဟာ မူလကတည်းက Max Supply အနေနဲ့ (၂၁) သန်းမှာ ကန့်သတ်ထားပြီး၊ အဲ့ဒီထဲက Deadcoin တွေ နှုတ်လိုက်ရင် ထပ်ပြီးတော့ လျော့သွားဦးမှာပါ။ တစ်ကယ်တော့ ဒီလိုလျော့သွားလေ ပိုရှားပါးပြီး ပိုအဖိုးတန်လာလေလို့လည်း ဆိုနိုင်ပါတယ်။

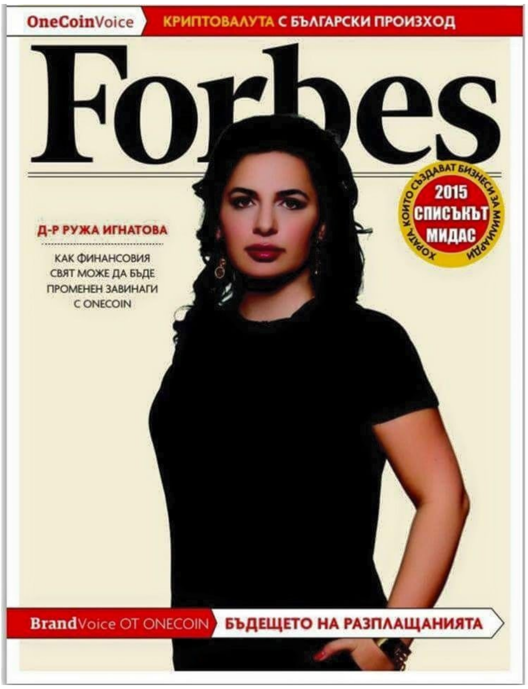
Cryptocurrency မှာ ကွိုင်တွေကို Burn လုပ်တယ်ဆိုတဲ့ သဘောသဘာဝ တစ်ခုလည်း ရှိပါသေးတယ်။ တချို့ Cryptocurrency တွေက အစပိုင်းမှာ စတင်လည်ပါတ်ဖို့အတွက် တီထွင်သူတွေ ကြိုတူးပြီး Pre-Mine လုပ်ထားတဲ့ ကွိုင်အများအပြား ရှိပေမယ့် နောက်ပိုင်းမှာ အဲ့ဒီလို ကြိုထုတ်ထားတဲ့ ကွိုင်တွေကို ပြန်ပြီးတော့ ဖျောက်ပေးကြတာတွေ ရှိပါတယ်။ အဲ့ဒီလိုလုပ်တာကို ကွိုင်တွေ Burn လုပ်တယ်လို့ ပြောကြတာပါ။ ဖျောက်ပေးတယ်ဆိုတာ Delete နှိပ်ပြီး ဖျက်လိုက်တာ မဟုတ်ပါဘူး။ Blockchain ထဲက Data ကို အဲ့လို ဖျက်လို့ မရပါဘူး။ ပြန်ထုတ်ယူလို့ မရနိုင်တဲ့၊ <u>အမှန်တစ်ကယ် မရှိတဲ့ Address ထဲကို ဖျက်ချင်တဲ့ ကွိုင်တွေ လွှဲပို့လိုက်တာပါ</u>။ ဒါဆိုရင် ပြန်ယူလို့မရနိုင်တော့ဘဲ အပြီးပျောက်သွားတာပါပဲ။

ဒါနဲ့ဆက်စပ်ပြီး တစ်ဆက်တည်း သတိထားရမှာက Bitcoin အပါအဝင် Cryptocurrency တွေကို လွှဲပို့တဲ့အခါ Address လိပ်စာ မမှားဖို့ အလွန်အရေးကြီးပါတယ်။ <u>လိပ်စာမှားရင် ပြန်ရတော့မှာ မဟုတ်လို့ပါ</u>။ ဘယ်သူမှ မရလိုက်ဘဲ ဆုံးသွားတဲ့ Deadcoin တွေပဲ ဖြစ်သွားပါလိမ့်မယ်။

OneCoin

Bitcoin ကို တချို့ဝေဖန်ကြသူတွေက တစ်ကယ်မရှိတဲ့အရာတစ်ခုကို မက်လုံးပေးပြီး လူတွေဆီက ငွေတွေလိမ်ယူနေတဲ့ Ponzi Scheme လို့ ဆိုကြပါတယ်။ Bitcoin က Network ထဲမှာ အမှန်တစ်ကယ်ရှိနေပြီး လက်တွေ့အသုံးလည်း ဝင်ပါတယ်။ တစ်ကယ်လည်းမရှိဘဲနဲ့ လူတွေကိုမက်လုံးပေးပြီး ငွေတွေလိမ်လည်သွားတာကတော့ OneCoin ပဲ ဖြစ်ပါတယ်။

Dr. Ruja လို့ခေါ်တဲ့ ဘူလ်ဂေးရီးယားနိုင်ငံသူ Ph.D ဘွဲ့ရ အမျိုးသမီးတစ်ဦးရဲ့ အကြံညာဏ်တွေပါ။ လန်ဒန်မြို့က ဝင်ဘလေကွင်းလို အထင်ကရနေရာမျိုးကြီးမှာ လူစုလူဝေး ပွဲကြီးတွေလုပ်ပြီး OneCoin အကြောင်း အကြီးအကျယ် ဟောပြောခဲ့ပါသေးတယ်။ ခပ်သေးသေးလုပ်သွားတာ မဟုတ်ပါဘူး။ တစ်ကယ့် အကြီးကြီး လုပ်သွားတာပါ။ Google မှာ Dr. Ruja လို့ ရှာလိုက်ရင် Forbes မဂ္ဂဇင်း မျက်နှာဖုံးမှာ သူ့ပုံနဲ့ တွေ့ရပါလိမ့်မယ်။ တစ်ကယ့် Forbes မဂ္ဂဇင်းကြီးရဲ့ မျက်နှာဖုံးမှာ ပါခဲ့တာ မဟုတ်ပါဘူး။ Forbes Bulgaria မှာ သူ့ပုံကို အခပေးပြီး ကြော်ငြာထည့်ခဲ့တာပါ။ ဒါပေမယ့် ရုတ်တရက် Search Result မှာကြည့်လိုက်ရင် တစ်ကယ့် Forbes မဂ္ဂဇင်းကြီးကပဲ သူ့ပုံကို မျက်နှာဖုံးပုံ တင်သလိုလို ထင်ရပါတယ်။ နာမည်ကြားလိုက်ယုံနဲ့ ရှိန်သွားအောင်၊ ရှာကြည့်လိုက်ရင် ယုံမိသွားအောင် လုပ်ထားတာက အတော်ပိရိပါတယ်။



OneCoin ရဖို့အတွက် Mine တစ်ကယ် မတူးရပါဘူး။ ကွိုင်ပုံစံ ဒင်္ဂါးလေးတွေနဲ့ ဒီဇိုင်းလုပ်ထားတဲ့ Package တွေ ဝယ်ရပါတယ်။ တစ်ဦးနဲ့တစ်ဦး အသိတွေ၊ အမျိုးတွေကနေ တစ်ဆင့်ခြင်း လက်ဆင့်ကမ်း ရောင်းရပါတယ်။ ဒီလိုလက်ဆင့်ကမ်း ရောင်းရတယ် ဆိုကတည်းက ဘာလဲဆိုတာ သဘောပေါက်ပါလိမ့်မယ်။ တစ်ထုတ်ကို ယူရို (၁၀၀) ကနေ (၁၀၀,၀၀၀) ကျော်အထိ လယ်ဗယ်အဆင့်တွေ ခွဲပြီးတော့ ရောင်းတာပါ။ ဒီအတွက် Exchange တွေဘာတွေ ထောင်ပြီး အဲ့ဒီအထုပ်ထဲက ကွိုင်တွေကို ယူရိုငွေနဲ့ ပြန်လဲယူလို့ ရအောင်ထိ လုပ်ပေးထားပါတယ်။

မရိုးသားတဲ့ Exchange ဖြစ်တဲ့အတွက် ဈေးတွေကို အမျိုးမျိုးပြပြီး လူတွေ လောဘ တက်သထက် တက်အောင်ပဲ လုပ်မှာပါပဲ။ ဥပမာ – ယူရို (၁၀၀) နဲ့ဝယ်လိုက်တဲ့ OneCoin ကို တစ်လလောက်နေတော့ သွားရောင်းတာ ယူရို (၂၀၀၀) တောင် ရတယ်ဆိုရင် ထောပြီလို့ တွေးကြမှာပါပဲ။ ဒီလောက်မြတ်နေတော့ အိမ်တိုင်ပါ ချွတ်ရောင်းပြီး ဝယ်ရင်းကြစို့ ဆိုတာမျိုးထိ ဖြစ်လာတော့တာပါပဲ။ တစ်ကယ်လည်း ရှိသမျှရောင်းချပြီး ထည့်တဲ့သူတွေ ရှိလာပါတယ်။ ဒီနည်းနဲ့ ကမ္ဘာအနှံ့အပြား၊ နိုင်ငံအသီးသီးက လူတွေဆီကနေ OneCoin ထဲကို ဒေါ်လာ (၁၅) ဘီလီယံလောက်ထိ ဝင်သွားတာပါ။

၂၀၁၆ ခုနှစ်မှာ Maintenance လုပ်ဖို့ဆိုတဲ့ အကြောင်းပြချက်နဲ့ Exchange ကို (၂) ပါတ်လောက် ပိတ်ခဲ့ပါသေးတယ်။ ပြန်ဖွင့်ချိန်မှာ ဘာမှ မဖြစ်ခဲ့ပေမယ့် ၂၀၁၇ ခုနှစ်ထဲ မှာတော့ ဘာမပြောညာမပြော ရုတ်တရက် အပြီးပိတ်ချ လိုက်ပါတော့တယ်။ OneCoin ဝယ်ရင်းထားသူတွေလည်း ထည့်ထားတဲ့ငွေ ပြန်မရတော့ဘဲ အကုန်ဆုံးတော့တာပါပဲ။

Dr. Ruja ကတော့ အဲ့ဒီအချိန်မှာ ရုတ်တရက် လုံးဝ ပျောက်ကွယ်သွားပါတော့တယ်။ ပြန်ပေးပဲ ဆွဲခံရသလို၊ လုပ်ကြံပဲ ခံရသလိုလို သတင်းထွက်အောင် လုပ်ထားပေမယ့် ထွက်ပြေးသွားတာ ဖြစ်ဖို့များပါတယ်။ မကြာခင်မှာပဲ FBI က Dr. Ruja နဲ့ အပေါင်းအပါတွေကို လိမ်လည်မှု၊ ငွေကြေးခဝါချမှုတွေနဲ့ ဖမ်းဝရမ်းထုတ်ခဲ့ပါတယ်။ ဂရိနိုင်ငံကို သွားဖို့ လေယာဉ်လက်မှတ် ဝယ်ထားတာဟာ Dr. Ruja ရဲ့ နောက်ဆုံးမှတ်တမ်းပါပဲ။ တစ်ကယ်ပဲ သွားခဲ့ပြီး ဂရိမှာ ဇာတ်မြုပ်နေသလား၊ ဘူလ်ဂေးရီးယားနိုင်ငံတစ်နေရာရာမှာပဲ ရုပ်ဖျက်ပြီး ပုန်းနေသလားတော့ ဘယ်သူမှ မသိကြပါဘူး။ လက်ရှိမှာ အမှုဟောင်းတွေအတွက် ထောင် (၁၄) လ ဆိုင်ငံ့ပြစ်ဒဏ်ချခံထားရပြီး OneCoin အတွက် စွဲချက်တင်ထားတဲ့ ပြစ်မှုတွေထင်ရှားရင် ထောင်ဒဏ် အနှစ် (၉၀) လောက်ထိကျမှာပါ။ ပြန်ပေါ်လာဦးမလား၊ ဖမ်းမိမလား ဆိုတာတော့ စောင့်ကြည့်ကြရပါဦးမယ်။

မှတ်ချက် ။ ။ ဒီနေရာမှာ One ဆိုတဲ့ အသုံးအနှုန်းတွေ့တိုင်းတော့ OneCoin လို့ မယူဆပါနဲ့ဦး။ Harmony One လို့ခေါ်တဲ့ Cryptocurrency အမှန်တစ်ခုလည်း ရှိပါသေးတယ်။ Harmony ဟာ နည်းပညာအဆင့်မြင့်ပြီး စိတ်ဝင်စားစရာ Cryptocurrency တစ်ခုပါ။ လက်ရှိ ဈေးကွက်တန်ဖိုး ဒေါ်လာသန်း (၆၀၀) ကျော်ထိ ရှိနေပြီး ONE ကို Currency Code အနေနဲ့ အသုံးပြုပါတယ်။

Bitconnect

နောက်ထပ် အလားတူ လိမ်လည်မှုတစ်ခုကတော့ Bitconnect ပါ။ Bitconnect ဟာ Bitcoin ချေးငှားတဲ့ နည်းပညာဖြစ်ပြီး BCC လို့ခေါ်တဲ့ Bitconnect Coin ကို ဝယ်ပြီး သိမ်းထားရင် အတိုးပေးမယ်ဆိုတဲ့ သဘောပါ။ သူလည်းပဲ တစ်ဦးနဲ့တစ်ဦး လက်ဆင့်ကမ်းပြီး ဆင့်ပွားရောင်းတဲ့နည်းကို သုံးပါတယ်။ ပြီးတော့ တစ်နေ့ 1% ထိ ထပ်တိုး အတိုးကို နေ့စဉ်ကျိမ်းသေ ရမယ်ဆိုတဲ့ မဖြစ်နိုင်တဲ့ ပမာဏကို ပေးထားတာပါ။

ဝယ်ထားရင် ကျိမ်းသေ မြတ်မယ်တို့၊ ထည့်ထားရင် ကျိမ်းသေ အတိုးရမယ်တို့ဆိုတဲ့ ကျိမ်းသေ တွေက တော်တော်လေး ကြောက်ရပါတယ်။ ငွေကို လွယ်လွယ်လိုချင်မိသူတွေကတော့ ဒီလိုအလိမ်အညာတွေနဲ့ တွေ့ရင် ခံရမှာပါပဲ။

တိုတိုပြောရရင် Bitconnect ဟာ လူတွေဆီက ငွေကိုလက်ခံယူနေပေမယ့် ဘယ်မှာမှ မှတ်ပုံတင်ထားခြင်း မရှိတဲ့ တရားမဝင် အဖွဲ့အစည်းပါ။ ဒါကြောင့်လည်း သက်ဆိုင်ရာ အာဏာပိုင်တွေက (၂၀၁၈) ခုနှစ်ထဲမှာ အချိန်မီ ဝင်စီးပြီး ငွေရင်းထည့်ထားသူတွေကို ပြန်အမ်းပေးနိုင်ခဲ့လို့ တော်သေးတယ်လို့ ဆိုရပါမယ်။ Bitconnect ရဲ့ အိန္ဒိယနိုင်ငံ ဒေသခေါင်းဆောင်လို့ ယူဆကြတဲ့ Divyesh Darji ဆိုသူကိုတော့ ဒေလီမြို့မှာ ဖမ်းဆီးရမိခဲ့ကြပါတယ်။

Divyesh Darji ဟာ Regal Coin ဆိုတဲ့ နောက်ထပ် Cryptocurrency လိမ်လည်မှုတစ်ခုနဲ့လည်း ဆက်စပ်နေပါသေးတယ်။ ပြီးတော့ စောစောကပြောခဲ့တဲ့ Dr. Ruja ဟာလည်း OneCoin မတိုင်ခင်က BigCoin ဆိုတဲ့နောက်ထပ် Cryptocurrency လိမ်လည်မှုတစ်ခုနဲ့ ဆက်စပ်နေခဲ့ပါတယ်။

ငွေကြေးနဲ့ပက်သက်တဲ့ ကိစ္စတွေဖြစ်နေလို့ ဒီလိုမျိုး အလိမ်အညာတွေကလည်း အများကြီးပဲ ရှိနေတာပါ။ တော်တော်လေး သတိထားဖို့ လိုအပ်ပါလိမ့်မယ်။ ဒီနေရာမှာ **DYOR** လို့အတိုကောက် ခေါ်ကြတဲ့ Do Your Own Research က အလွန် အရေးကြီးပါတယ်။ နည်းပညာ သိချင်ယုံသက်သက်ဆိုရင် ပြဿနာမရှိပါဘူး။ ကိုယ့်ငွေ အရင်းပြုဖို့ထိ စဉ်းစားလာရင်တော့ DYOR ကို ကောင်းကောင်း လုပ်ရပါလိမ့်မယ်။ စာရေးသူပြော လို့လည်း ချက်ခြင်းမယုံသင့်ပါဘူး။ အမျိုးတွေ အသိတွေ သူငယ်ချင်းတွေ ပြောလို့လည်း ချက်ခြင်း မယုံ သင့်ပါဘူး။ သေချာအောင် ကိုယ်တိုင် အသေးစိတ် လေ့လာပြီးမှ ဆုံးဖြတ်ဖို့ လိုအပ်ပါလိမ့်မယ်။

စာရေးသူကတော့ အခုဒီစာဖတ်နေသူတွေကို Bitcoin အပါအဝင် Cryptocurrency တွေမှာ ရင်းနှီးမြှုပ်နှံဖို့ တိုက်တွန်း ပြောဆိုနေတာ မဟုတ်ပါဘူး။ ဒါပေမယ့် Bitcoin ဟာ စိတ်ချရတဲ့ နည်းပညာဆိုတဲ့သဘောမျိုး ကို ရှင်းပြနေတာဖြစ်လို့ သွယ်ဝိုက်တိုက်တွန်းမိသလို ဖြစ်နေမှာကိုတော့ စိုးရိမ်မိပါတယ်။ နည်းပညာကို သိအောင်ပဲ ပြောပြတာပါ။ Bitcoin အပါအဝင် Cryptocurrency တွေမှာ ရင်းနှီးမြှုပ်နှံဖို့ တိုက်တွန်းခြင်း လုံးဝမဟုတ်ပါဘူးလို့ အတိအလင်း ပြောချင်ပါတယ်။ တစ်ဆက်ထဲမှာပဲ ဒီကဏ္ဍမှာ ငွေကြေးဆုံးရှုံးနစ်နာ နိုင်တဲ့၊ ကြောက်ဖို့အလွန်ကောင်းတဲ့၊ အလိမ်အညာတွေလည်း ရှိတယ်ဆိုတာကို သတိပေးချင်လို့ အခုလို ဒီ အဖြစ်အပျက်တွေကို ထည့်ပြောပြနေတာပါ။

QuadrigaCX

ဒီအကြောင်းတွေနဲ့ ပက်သက်ပြီး နောက်တစ်ခုအနေနဲ့ ထည့်ပြောချင်တာကတော့ ကနေဒါအခြေစိုက် Quardriga CX လို့ခေါ်တဲ့ Cryptocurrency Exchange အကြောင်းပဲဖြစ်ပါတယ်။ ဒီ Exchange ကတော့ တရားဝင် Exchange တစ်ခုအနေနဲ့ အလုပ်လုပ်ခဲ့တာပါ။ အများပိုင်ကုမ္ပဏီအနေနဲ့ ကနေဒါ Stock Exchange မှာ တင်ဖို့ထိ ပြင်ဆင်ဖြစ်ခဲ့ပါသေးတယ်။

အစပိုင်း အခြေအနေ သိပ်မကောင်းလှပေမယ့် ၂၀၁၄ ခုနှစ်အတွင်း ကနေဒါဒေါ်လာ (၇.၄) မီလီယံ ပမာဏ အရောင်းအဝယ် လုပ်ပေးနိုင်ခဲ့ပါတယ်။ ၂၀၁၇ ခုနှစ်မှာ Bitcoin ဈေးတွေ ထိုးတက်သွားတဲ့အတွက် ကနေ ဒါ ဒေါ်လာ (၁.၂) ဘီလီယံဖိုးအထိ အရောင်းအဝယ် လုပ်ပေးနိုင်ခဲ့ပါတယ်။ ဒါပေမယ့် ၂၀၁၈ ခုနှစ် Bitcoin ဈေးတွေ ပြန်ကျချိန်မှာတော့ ငွေပြန်ထုတ်ရခက်တဲ့ ပြဿနာတွေ စလာတော့တာပါပဲ။ ဒီအချိန်မှာ လိမ် ပြေးဖို့ ကြိုးစားနေတာတော့ ဟုတ်ချင်မှ ဟုတ်ပါလိမ့်မယ်။ အဓိကအားဖြင့် စီမံခန့်ခွဲမှု အားနည်းချက် တွေကြောင့် အခက်အခဲတွေ များနေတာလို့ ဆိုနိုင်ပါတယ်။

တစ်ကယ့်ပဟေဠိကတော့ ၂၀၁၈ ခုနှစ်၊ ဒီဇင်ဘာလမှာ QuadrigaCX ရဲ့ တည်ထောင်သူ Gerald Cotten ရုတ်တရက် သေဆုံးသွားခြင်း ဖြစ်ပါတယ်။ သူ့မိန်းမရဲ့ ပြောပြချက်နဲ့ ဆေးရုံသေစာရင်းအရ အိန္ဒိယနိုင်ငံကို အလည်အပါတ် ခရီးသွားနေစဉ်မှာ ရုတ်တရက် နှလုံးရောဂါဖောက်ပြီး အိန္ဒိယမှာပဲ သေဆုံးသွားတယ်လို့ ဆိုပါတယ်။ သူနဲ့အတူ ကနေဒါ ဒေါ်လာ သန်း (၂၅၀) လောက် တန်ဖိုးရှိတဲ့ Customer (၁) သိန်းကျော်ရဲ့ Cryptocurrency တွေ ပါသွားပါတော့တယ်။

သူနဲ့အတူ ပါသွားတယ်ဆိုတာက ဒီလိုပါ။ Exchange တွေက Customer တွေ အရောင်းအဝယ်လုပ်ဖို့ ပို့ထားတဲ့ Cryptocurrency တွေကို စိတ်ချရအောင် Offline Cold Wallet အနေနဲ့ သိမ်းထားကြလေ့ ရှိပါတယ်။ Online မှာ ထားရင် ဟက်ခံရတာတွေဘာတွေ ရှိတတ်တဲ့အတွက် ဆုံးရှုံးမှာ စိုးလို့ပါ။ အွန်လိုင်းမှာ ကိန်းဂဏန်းတွေသာ ရှိပြီး တစ်ကယ့် Cryptocurrency တွေရဲ့ Private Key တွေက Hardware Wallet (သို့မဟုတ်) စာရွက်မှာ ချရေးပြီး လုံခြုံရာမှာ သိမ်းဆည်းထားကြတဲ့ သဘောပါ။ အဲ့ဒီလိုသိမ်းဆည်းထားတဲ့ Password ကို Gerald Cotten တစ်ဦးထဲသာ သိတဲ့အတွက် သူသေဆုံးသွားတဲ့အခါ အဲ့ဒီ Cryptocurrency တွေလည်း ပျောက်ပျက်သွားတော့တာပါပဲ။

ဒီဖြစ်စဉ်ကြောင့် QuadrigaCX လည်း Customer တွေကို ပျောက်သွားတဲ့ Cryptocurrency တွေ ပြန်မအမ်းနိုင်တော့လို့ ဒေဝါလီ ခံသွားရပါတယ်။ အလွန်သံသယရှိဖွယ် ဖြစ်ရပ်ဖြစ်တဲ့အတွက် Gerald Cotten သေသွားတယ်ဆိုတာကို လူတွေက မယုံကြပါဘူး။ ရုတ်တရက်ကြီး အရမ်းတိုက်ဆိုင်နေသလို အိန္ဒိယဆိုတာ စာရွက်စာတမ်း အတုလုပ်ဖို့ မခက်တဲ့နေရာ ဖြစ်နေပါတယ်။ သေစာရင်းစာရွက်မှာပါတဲ့ နာမည်က စာလုံးပေါင်းလည်း မှားနေပါသေးတယ်။

प्रारूप संख्या 6
FORM NO. 6

राजस्थान सरकार
Government of Rajasthan

आर्थिक एवं सांख्यिकी निदेशालय
Directorate of Economics & Statistics

मृत्यु प्रमाण पत्र
DEATH CERTIFICATE

(जन्म और मृत्यु रजिस्ट्रीकरण अधिनियम,1969 की धारा 12/17 और राजस्थान जन्म और मृत्यु रजिस्ट्रीकरण नियम, 2000 के नियम 8/13 के अधीन जारी किया गया)

(Issued under Section 12/17 of the Registration of Births and Deaths Act,1969 and Rule 8/13 of the Rajasthan Registration of Births and Deaths Rules, 2000)

यह प्रमाणित किया जाता है कि निम्नलिखित सूचना मृत्यु के मूल अभिलेख से ली गयी है जो कि (स्थानीय क्षेत्र / स्थानीय निकाय)........ तहसील/खण्ड........जिला........राज्य/संघ राज्य........ का रजिस्टर

This is to certify that the following information has been taken from the original record of death which is the register for (Local area / Local body) SANGANER ZONE of Tehsil / Block xxxx of District JAIPUR of State / Union Territory RAJASTHAN.

नाम/Name : GERALD WILLIAM COTTAN

लिंग/Sex : MALE

मृतक का आधार नंबर /Deceased Aadhar No :

मृत्यु का स्थान/Place of Death :

मृत्यु की तिथि / Date of Death : 09/12/2018

FORTIS ESCORTS HOSPITAL, J.L.N. MARG, MALVIYA NAGAR, JAIPUR

Gerald Cotten တစ်ကယ်သေသွားသလား၊ ငွေတွေယူပြီး သေချင်ယောင်ဆောင်သွားသလား ဆိုတာတော့ အခုချိန်ထိ ပဟေဋ္ဌိတစ်ခု ဖြစ်နေဆဲပါပဲ။

ICO Frauds

Bitcoin ရဲ့ အောင်မြင်လာမှုနဲ့အတူ နောက်ဆက်တွဲ ပေါ်လာတာကတော့ အလားတူ Blockchain အခြေပြု နည်းပညာတွေ၊ Cryptocurrency မူကွဲတွေပါပဲ။ တစ်ကယ်တော့ Bitcoin ရဲ့ နည်းပညာကို အသုံးပြုပြီး မည်သူမဆို ကိုယ်ပိုင် Cryptocurrency တီထွင်လို့ ရနိုင်ပါတယ်။ ဒါမှမဟုတ် အိုင်ဒီယာ လောက်ကိုပဲ ယူပြီး ပိုကောင်းတဲ့ ကိုယ်ပိုင်အိုင်ဒီယာသစ်တွေ ကိုယ်ပိုင်နည်းပညာတွေ ထပ်ပေါင်းထည့်ပြီး တော့လည်း တီထွင်လို့ ရနိုင်ပါတယ်။ ဒီလိုတီထွင်ထားတဲ့ Cryptocurrency ကို ဗဟိုပြုပြီး လည်ပါတ်တဲ့ လုပ်ငန်းတွေ ထူထောင်မယ်ဆိုရင် ထူထောင်လို့ ရနိုင်ပါတယ်။

အခုဆိုရင် Cryptocurrency မှုကွဲတွေ များလွန်းအားကြီးလို့ ဖောင်းပွတဲ့အဆင့်ကိုတောင် ရောက်နေတယ်လို့ ဆိုနိုင်ပါတယ်။ ဒီမူကွဲတွေကို ပေါင်းစုပြီး Altcoin လို့ ခေါ်ကြပါတယ်။ အခုဒီစာရေးနေချိန်မှာ Altcoin ပေါင်း (၇,၅၀၀) လောက်ထိ ရှိနေပါတယ်။ တချို့က အမှန်တစ်ကယ် အသုံးဝင်တဲ့ စိတ်လှုပ်ရှားဖွယ် အိုင်ဒီယာသစ် နည်းပညာသစ်တွေကို မိတ်ဆက်ဖော်ထုတ်လာကြတဲ့ အမှန်အကန်တွေပါ။ တချို့ကတော့ ငွေလွယ်လွယ်ရမလားလို့ ပေါ်ပင်လိုက်လုပ်တဲ့ အတုအယောင်တွေပါ။ တချို့ကတော့ စကတည်းက လူတွေဆီက ငွေတွေလိမ်ယူဖို့ ရည်ရွယ်ချက်နဲ့ကို လုပ်ကြတာပါ။

နည်းပညာသစ်တစ်ခုပဲဖြစ်ဖြစ် လုပ်ငန်းသစ်တစ်ခုပဲဖြစ်ဖြစ် ထူထောင်ရတာ မလွယ်ပါဘူး။ ငွေအရင်းအနှီးလိုပါတယ်။ ကိုယ့်ရဲ့ အိုင်ဒီယာကို ချပြပြီး ဘဏ်တွေ၊ တစ်ကိုယ်တော် ရင်းနှီးမြှုပ်နှံသူ Angel Investor တွေ၊ Venture Capital တွေဆီက တည်ထောင်မယ့် ကုမ္ပဏီရဲ့ ရှယ်ယာကိုပေးပြီး ငွေအရင်းအနှီးကို ရယူကြရလေ့ရှိပါတယ်။ စတော့ရှယ်ယာဈေးကွက်ထဲ မရောက်ခင်ကတည်းက ကုမ္ပဏီရှယ်ယာကို ကြိုဝယ်ယူပြီး အရင်းထုတ်ပေးလိုက်တဲ့ သဘောမျိုးပါ။

Cryptocurrency လုပ်ငန်းသစ်တွေ အတွက်ကတော့ ထူးခြားပါတယ်။ ငွေအရင်းအနှီးရဖို့အတွက် အဲ့ဒီလိုကုမ္ပဏီရဲ့ ရှယ်ယာကိုကြိုပေးပြီး ငွေရင်းယူလို့လည်း ရနိုင်ပါတယ်။ နောက်တစ်နည်းကတော့ တီထွင်မယ့် Cryptocurrency ကွိုင်တွေကို ကြိုရောင်းပေးပြီးတော့လည်း ငွေရင်းယူလို့ ရနိုင်ပါသေးတယ်။

ဒီသဘောသဘာဝကို Initial Coin Offering (ICO) လို့ ခေါ်ကြပါတယ်။ ရင်းနှီးမြှုပ်နှံလိုသူတွေက ရှယ်ယာကိုဝယ်ပြီး ငွေရင်းထုတ်ပေးတာ မဟုတ်တော့ပါဘူး။ တီထွင်မယ့် Cryptocurrency ကို ဈေးကွက်ထဲ မရောက်ခင်ကတည်းက ကြိုတင်ဝယ်ယူပြီး ငွေရင်းထူထောင် ပေးလိုက်တာမျိုးပါ။

ရှယ်ယာကိုဝယ်ပြီး ငွေရင်းပေးတဲ့အခါ နောက်ပိုင်းမှာ ကုမ္ပဏီကြီးမားလာလို့ ဈေးကွက်တန်ဖိုး တက်လာတဲ့အခါ ရှယ်ယာဈေးတွေလည်း လိုက်တက်လာမှာမို့လို့ ရင်းနှီးမြှုတ်နှံသူအတွက် အကျိုးရှိနိုင်ပါတယ်။ Risk အနေနဲ့ ကတော့ မျှော်မှန်းသလို တိုးတက်မလာတာမျိုးလည်း ဖြစ်သွားနိုင်တာပါပဲ။

ကွိုင်တွေကို ကြိုဝယ်ပြီး ငွေရင်းပေးရတာလည်း ဒီသဘောပါပဲ။ သက်ဆိုင်ရာ ကုမ္ပဏီက တင်ပြတဲ့ အိုင်ဒီယာကိုကြည့်ပြီး၊ သူ့ကွိုင်ဟာ နောင်တစ်ချိန်မှာ ဆယ်ဆ၊ အဆတစ်ရာ တန်ကြေးတက်လာနိုင်ခြေ ရှိတယ်ဆိုတဲ့ မျှော်မှန်းချက်မျိုးနဲ့ ကြိုတင်ဝယ်ယူကြတာပါ။

ရမယ့် အကျိုးအမြတ် ကြီးသလို Risk ကလည်း ကြီးပါတယ်။ မျှော်မှန်းထားသလို နောင်တစ်ချိန် ဈေးတက်လာတာ ဖြစ်နိုင်သလို၊ တစ်ပြားမှ မတန်တော့တာမျိုးလည်း ဖြစ်သွားနိုင်တဲ့ အတွက်ကြောင့်ပါ။

ဒီနေရာမှာ ကြားဖြတ် မှတ်သားသင့်တာကတော့ Coin ဆိုတဲ့အသုံးအနှုန်းနဲ့ Token ဆိုတဲ့အသုံးအနှုန်းတို့ရဲ့ ကွဲပြားမှုပါ။ Mine လုပ်လိုက်လို့ Coinbase ကနေ အလိုအလျောက် ထွက်လာတဲ့ အရာကို Coin လို့ သုံးကြပြီး ICO အတွက်ပဲ ဖြစ်ဖြစ်၊ တစ်ခြား လိုအပ်ချက်ကြောင့်ပဲဖြစ်ဖြစ် တမင် ဖန်တီးယူလိုက်လို့ ထွက်လာတဲ့ ငွေကြေးကို Token လို့ သုံးကြပါတယ်။ ဒီနှစ်မျိုးကို ခပ်ဆင်ဆင် အသုံးပြုကြတာ မကြာခဏ တွေ့ရနိုင်ပါတယ်။ လိုရင်းအချုပ်အနေနဲ့ Coin ဆိုတာ Coinbase ကနေ Mine တူးလို့ ထွက်လာတာဖြစ်ပြီး Token ဆိုတာကတော့ Mine တူးစရာမလိုဘဲ ဒီအတိုင်း ဖန်တီးယူထားတာလို့ မှတ်နိုင်ပါတယ်။

ရှေ့ပိုင်းမှာ Bitcoin ကနေ အကျိုးအမြတ်တွေ အများကြီးရထားတဲ့ နမူနာ ရှိထားတဲ့အတွက် ICO တွေအပေါ်မှာ လူစိတ်ဝင်စားမှု အလွန်များပြားပါတယ်။ လုပ်ငန်းထူထောင်ဖို့ ငွေရင်း လွယ်လွယ်နဲ့ မြန်မြန်ရချင်တဲ့သူတွေက စိတ်ဝင်စားကြသလို၊ အမြတ်များများ ပြန်ရမယ့် အလားအလာတွေရှိလို့ ရင်းနှီးမြှုပ်နှံသူတွေကလည်း စိတ်ဝင်စားကြတာပါ။ စစ်တမ်းတစ်ခုအရ ၂၀၁၆ ခုနှစ် ဇန်နဝါရီလ ကနေ ၂၀၁၉ ခုနှစ် ဩဂုတ်လအထိ ICO ကနေ ရတဲ့ စုစုပေါင်း ရင်းနှီးမြှုပ်နှံငွေ ပမာဏဟာ ဒေါ်လာ (၁၃) ဘီလီယံထိ ရှိနေပါတယ်။ ပြဿနာကတော့ အဲ့ဒီ ICO တွေရဲ့ အများစု ဖြစ်တဲ့ (၇၈%) လောက်က ငွေလွယ်လွယ်ရဖို့နဲ့ လူတွေရဲ့ ငွေတွေကို လိမ်ယူဖို့ ရည်ရွယ်ထားတဲ့ အတုအယောင်တွေ ဖြစ်နေတာပါပဲ။

ICO တွေမှာ ရင်းနှီးမြှုပ်နှံကြတာ၊ ရင်းနှီးမြှုပ်နှံမှု လုပ်ငန်းတွေချည်းပဲ မဟုတ်ပါဘူး။ သာမန်လူအများလည်း ပါကြပါတယ်။ သေသေချာချာ ရေရေရာရာ မသိဘဲ ကျိမ်းသေမြတ်မယ်ဆိုပြီး အဆွယ်ကောင်းလို့ ICO အနေနဲ့ ရောင်းပေးနေချိန် ကွိုင်တချို့ ဝင်ဝယ်ထားတယ် ဆိုတာမျိုးတွေ ရှိကြပါတယ်။ ဒါကြောင့် အလိမ်ခံရတဲ့အခါ အဲ့ဒီသာမန်လူတွေလည်း ခံကြရတော့တာပါပဲ။ အပြောကောင်းကောင်းနဲ့ ကွိုင်တွေကို ကြိုရောင်း၊ ရတဲ့ငွေတွေယူပြီး ကိုယ်ယောင်ဖျောက် ထွက်ပြေးသွားတဲ့ ဖြစ်စဉ်တွေမှ အများကြီးပါ။

ဒီလိုထွက်ပြေးတဲနည်းအပြင် Pump and Dump လို့ခေါ်ကြတဲ့ နည်းလည်း ရှိပါသေးတယ်။ သူကတော့ အစပိုင်း ဟုတ်တိပတ်တိ အလုပ်တွေ တစ်ကယ်လုပ်ပြ၊ ဈေးတွေတက်အောင် နည်းလမ်း အမျိုးမျိုးနဲ့ ဆွဲခေါ်ပါသေးတယ်။ ဈေးတွေ တစ်ကယ်တက်လာပြီဆိုတော့မှ ကွိုင်တွေအများကြီး ချရောင်းပြီး ငွေထုတ်ပိုက်ပြေးတဲ့နည်းပါ။ အစကတည်းက အမှန်တစ်ကယ် အလုပ်လုပ်ဖို့ အစီအစဉ်မရှိဘဲ ဒီလိုအခွင့်အရေးကို

ကြံ့စည်ကြသူတွေပါ။ သူဒီလို ချရောင်းပြေးတဲ့အတွက် အဲ့ဒီကွိုင်ရဲ့ ဈေးတွေလည်းထိုးဆင်းပြီး တစ်ခြားသူ တွေကတော့ အကုန်လုံး အရှုံးပေါ်ကုန်ကြရတာမျိုးပါ။ ဒီလိုကွိုင်အမျိုးအစားကို **Shitcoin** လို့ ခေါ်ကြပါ တယ်။ Shitcoin တွေ မကိုင်မိဖို့ လိုပါတယ်။

ဒါကြောင့် ICO လို့ဆိုရင် သေသေချာချာ စမ်းစစ်ဖို့ လိုပါလိမ့်မယ်။ သူ့ White Paper ကိုကြည့်ပြီး အလားအလာကောင်းတဲ့ အိုင်ဒီယာ ဟုတ်ရဲ့လား သုံးသပ်ရပါမယ်။ တည်ထောင်သူဟာ ယုံကြည်ရတဲ့သူ ဟုတ်ရဲ့လား။ တီထွင်မယ့် Cryptocurrency ဟာ Transparency ကောင်းရဲ့လား။ ဆိုလိုတာက Token ဘယ်လောက် ကြိုထုတ်မှာလဲ။ ကွိုင်ဘယ်လောက် ပမာဏကို Pre-Mine ကြိုလုပ်မှာလဲ။ တီထွင်သူနဲ့ အပေါင်းအပါတွေက အဲ့ဒီ ကွိုင်နဲ့ Token တွေရဲ့ ဘယ်လောက် ပမာဏကို ကိုင်ထားမှာလဲ။ ဘယ်အချိန်မှာ ပြောထားတဲ့ အိုင်ဒီယာ အလုပ်တစ်ကယ် စလုပ်မှာလဲ။ ကွိုင်တွေ မဖောင်းပွအောင် ဘယ်လို စီမံထားလဲ။ Mine တူးတဲ့သူတွေက ဘယ်သူတွေလဲ။ သူထွင်ပြီး သူတူးနေတာမျိုး ဖြစ်နေသလား။ Decentralize ရော တစ်ကယ် ဖြစ်ရဲ့လား။ စသည်ဖြင့် မေးစရာမေးခွန်းတွေ အများကြီးရှိပါလိမ့်မယ်။ ICO ကောင်းကောင်းမှာ ပါဝင်မိရင် အကျိုးများနိုင်သလောက်၊ မမှန်ကန်တဲ့ ICO မှာပါရင်တော့ အလိမ်ခံရပါလိမ့်မယ်။

ငွေကြေးကိစ္စမှာ သတိဆိုတာ ပိုတယ်မရှိပါဘူး။ ဒါကြောင့် ဒါတွေကို အရင်ကြိုပြောနေတာပါ။ ဒါပေမယ့် Bitcoin လိုမျိုး စနစ်တစ်ခု၊ ခေတ်တစ်ခုကို ပြောင်းသွားစေလောက်တဲ့ထိ အိုင်ဒီယာကောင်းတဲ့ နောက်တိုး Cryptocurrency Altcoin တွေလည်း အများကြီး ရှိနေပါသေးတယ်။ တချို့က Bitcoin ရဲ့ အားနည်းချက် တွေကို အဆင့်မြှင့်တင် ပြုပြင်ပြီး ထွက်ပေါ်လာကြပါတယ်။ တချို့က Bitcoin နဲ့မတူတဲ့ ချဉ်းကပ်ပုံကို အသုံးပြုကြပါတယ်။ တချို့ကတော့ Currency ဆိုတာထက် အများကြီး ပိုသွားပြီလို့ ဆိုရမယ့် အသုံးဝင်တဲ့ ဖြည့်စွက်အိုင်ဒီယာတွေ၊ နည်းပညာတွေ ပါဝင်ကြပါတယ်။

အဲ့ဒီအကြောင်းလေးတွေ ဒီစာအုပ်မှာ အကုန်စုံအောင်တော့ ဖော်ပြနိုင်မှာ မဟုတ်ပါဘူး။ အရေးပါပြီး သတိပြုသင့်တာလေးတွေကိုတော့ ရသလောက်ထည့်ပြီး ဆက်လက်ဖော်ပြသွားပါမယ်။

အခန်း (၆) – Altcoins များ

Bitcoin ထွက်ပေါ်လာပြီးနောက်မှာ ထပ်မံထွက်ပေါ်လာတဲ့ Altcoin ပေါင်း များစွာ ရှိနေပါတယ်။ အခုဒီစာရေးနေချိန်မှာ Altcoin ပေါင်း (၇,၅၀၀) ကျော်ထိ ရှိနေပါတယ်။ မနည်းမနောပါပဲ။ အဲ့ဒီထဲက တချို့က ပြီးခဲ့တဲ့အခန်းမှာ ပြောခဲ့သလို လူတွေရဲ့ငွေကို လိမ်ညာလှည့်ဖြားပြီး ယူဖို့ကြံထားတဲ့ Shitcoin သက်သက်တွေပါ။ ဘာမှ အသုံးမဝင်ပါဘူး။ တချို့ကတော့ Bitcoin ကို နမူနာယူပြီး ပြင်ဆင်ဖြည့်စွက်ချက်အချို့နဲ့ အတူ ထွက်ပေါ်လာကြတာပါ။ တချို့ကတော့ Bitcoin နဲ့ ဘာဆိုဘာမှ မဆိုင်တော့ပါဘူး။ တစ်ကယ့်ကို ဆန်းကျယ်ထူးခြားပြီး နည်းပညာလောကကို တစ်ခေတ်ဆန်းစေနိုင်လောက်တဲ့ တီထွင်မှုအသစ်တွေ ပါဝင်လာကြပါတယ်။ အဲ့ဒီလို ထူးခြားတဲ့ Altcoin အချို့အကြောင်းကို ရွေးထုတ်ဖော်ပြသွားမှာပါ။

Litecoin (LTC)

Litecoin ဟာ အစောဆုံးပေါ်ထွက်ခဲ့တဲ့ Altcoin တွေထဲက တစ်ခုပါ။ ၂၀၁၁ ခုနှစ်တုံးက အဲ့ဒီအချိန် Google မှာ အလုပ်လုပ်နေတဲ့ Charlie Lee လို့ခေါ်တဲ့ ဆော့ဖ်ဝဲအင်ဂျင်နီယာတစ်ဦးက Bitcoin ရဲ့ Source Code ကို ပွားယူ အခြေခံပြီး တီထွင်ခဲ့တာပါ။ Charlie Lee ဟာ နောက်ပိုင်းမှာ Coinbase Exchange ရဲ့ Engineering Director ဖြစ်လာခဲ့ပါတယ်။

Bitcoin လို Open Source ပရောဂျက်တွေဟာ ဒီလိုပါပဲ။ သူ့မူရင်း Source Code မှာ ဝိုင်းကူ ပါဝင်ပေးလို့ရသလို၊ လိုအပ်ရင် သတ်မှတ်ချက်များနဲ့အညီ ပွားယူလို့လည်း ရပါတယ်။ Litecoin ရဲ့ ရည်ရွယ်ချက်ကတော့ Bitcoin ရဲ့ တစ်စက္ကန့်မှာ Transaction (၆.၅) ခု ခန့်သာ ဆောင်ရွက်နိုင်ခြင်း ဆိုတဲ့ အကန့်အသတ် ပြဿနာကို ဖြေရှင်းဖို့ ဖြစ်ပါတယ်။ Silver to Bitcoin’s Gold ဆိုတဲ့ ဆောင်ပုဒ်နဲ့ လုပ်ခဲ့တာပါ။ ဆိုလိုတာက Bitcoin ကို အဖိုးတန်ရွှေလို့ သဘောထားပြီး Litecoin ကို ပိုပြီးတော့ ပေါ့ပေါ့ပါးပါး ဖလှယ်လို့ကောင်းတဲ့ ငွေလို့ သဘောထားစေချင်တာပါ။

Bitcoin ဟာ Max Supply အနေနဲ့ (၂၁) သန်းမှာ ကန့်သန့်ထားပေမယ့် Litecoin ရဲ့ Max Supply ကတော့ (၈၄) သန်း ဖြစ်ပါတယ်။ Proof of Work ကို ပြဖို့အတွက် Bitcoin ကို SHA-256 Hash ကို အသုံး မပြုဘဲ Scrypt လို့ခေါ်တဲ့ စက်စွမ်းအင်လိုအပ်ချက် ပိုနည်းတဲ့ Hash ကို သုံးထားပါတယ်။ Difficulty ကို လည်း လျှော့ထားတဲ့အတွက် Bitcoin လိုမျိုး (၁၀) မိနစ်တစ်ခါမှ Block အသစ် Confirm လုပ်တာ မဟုတ် တော့ပါဘူး။ (၂) မိနစ်ခွဲတစ်ခါ Block အသစ် Confirm လုပ်တာပါ။ Block ထည့်ပေးရင်ရတဲ့ ဆုကြေး ကတော့ အစပိုင်းမှာ 50 LTC ဖြစ်ပြီး Block ပေါင်း (၈၄၀,၀၀၀) ပြည့်တိုင်း ဆုကြေးတစ်ဝက်လျှော့ပါတယ်။

အခြေခံအားဖြင့် ထူးထူးထွေထွေ ဆန်းပြားတဲ့ Coin မဟုတ်ဘဲ Bitcoin ကို အခြေခံထားပြီး Bitcoin ထက် နည်းနည်းပိုမြန်တဲ့ Cryptocurrency ဖြစ်ပါတယ်။ လက်ရှိမှာ စုစုပေါင်း ဈေးကွက်တန်ဖိုး Market Cap ဒေါ်လာ (၉) ဘီလီယံကျော် ရှိနေပါတယ်။ Market Cap နဲ့စီလိုက်ရင် Cryptocurrency စာရင်းရဲ့ အဆင့် (၁၃) မှာရှိနေပါတယ်။

Dogecoin (DOGE)

Dogecoin ဟာ အဲ့ဒီအချိန်တုံးက မှိုလိုပေါက်ပြီး ဖောင်းပွနေတဲ့ Cryptocurrency တွေကို နောက်ပြောင်ကျီစယ်တဲ့သဘောနဲ့ Jackson Palmer လို့ခေါ်တဲ့ Adobe က အင်ဂျင်နီယာ တစ် ဦးနဲ့ Billy Markus လို့ခေါ်တဲ့ IBM က အင်ဂျင်နီယာတစ်ဦး တို့က ၂၀၁၃ ခုနှစ်မှာ တီထွင်ခဲ့တဲ့ Altcoin ဖြစ်ပါတယ်။ Coin ရဲ့ ရုပ်ပုံလိုဂို အနေနဲ့ အင်တာနက် Meme တွေမှာ သုံးလေ့ရှိတဲ့ ဂျပန်ခွေးမျိုးစိတ်ဖြစ်တဲ့ Shiba Inu ကို အသုံးပြုထားလို့ သူ့ကို Memecoin လို့လည်း ခေါ်ကြပါတယ်။

Litecoin ရဲ့ Source Code ကနေဆင်းသက်လာလို့ သူလည်းပဲ Bitcoin ရဲ့ တိုက်ရိုက်မျိုးဆက် တစ်ခုပါပဲ။ ဒါကြောင့် နောက်ပြောင်ကျီစယ်ပြီး ဖန်တီးထားပေမယ့် နည်းပညာက လက်တွေ့အသုံးချအဆင့် နည်း ပညာပါ။ Elon Musk လိုလူမျိုးကအစ Dogecoin ကို အသုံးချပြီး Cryptocurrency တွေကို မကြာခဏ အင်တာနက်မှာ နောက်ပြောင် ကျီစယ်လေ့ရှိလို့ လူအများစု ဘာရယ်မဟုတ် သဘောကျကြတဲ့ ကွိုင်တစ်ခု ပါ။ Cryptocurrency အမာခံတွေကတော့ မကြိုက်ကြပါဘူး။ အတည်အတန့် လုပ်နေတာကို လာပြောင် သလို ဖြစ်နေတယ်လို့ သဘောထားတယ် ထင်ပါတယ်။

စကတည်းက နောက်ပြောင်ကျီစယ်တဲ့ အရာဖြစ်လို့ Dogecoin ရဲ့ ဈေးအတက်အကျဟာ သူ့တန်ဖိုး အစစ်အမှန်ပေါ် အခြေခံခြင်းထက် ဆိုရှယ်မီဒီယာက Meme တွေပေါ်မူတည်ပြီး အတက်အကျ ဖြစ်နေတာက ပိုများပါတယ်။ သူ့ရဲ့ Market Cap က ဒေါ်လာ (၃၅) ဘီလီကျော်တောင် ရှိနေတာပါ။ Litecoin ထက်တောင် များပါသေးတယ်။

Dogecoin မှာ Max Supply မရှိသလို Block အသစ်ထည့်ဖို့ကိုလည်း (၁) မိနစ်တစ်ကြိမ်ထိ လျှော့ပေးထားပါတယ်။ ရမယ့် ဆုကြေးကလည်း Block တစ်ခုကို (၁၀,၀၀၀) ထိ ပေးထားတာပါ။ ဒီအချက်တွေကြောင့် အမှန်တစ်ကယ် အဖိုးတန်တဲ့ Coin လို့ ဆိုနိုင်ပါ့မလားဆိုတာတော့ စဉ်းစားစရာပါ။

နောက်ပိုင်းမှာ Shiba Inu (SHIB) ဆိုတဲ့အမည်နဲ့ပဲ Memecoin တစ်ခု ထပ်ပေါ်လာပြီး လက်ရှိ Market Cap ကလည်း ဒေါ်လာ (၃) ဘီလီယံကျော်ထိ ရှိနေပါတယ်။ Bitcoin အပါအဝင် Altcoin တွေရဲ့ လက်ရှိ ပေါက်ဈေးနဲ့ ဈေးကွက်အခြေအနေကို Coin Market Cap မှာ လေ့လာနိုင်ပါတယ်။

https://coinmarketcap.com

#	Name	Price	24h %	7d %	Market Cap	Volume(24h)	Circulating Supply	Last 7 Days
1	Bitcoin BTC Buy	$36,312.98	▲6.15%	▲24.52%	$682,135,904,327	$37,268,733,770 1,024,116 BTC	18,744,562 BTC	
2	Ethereum ETH Buy	$2,220.81	▲10.80%	▲28.10%	$259,193,691,016	$26,993,158,427 12,131,406 ETH	116,488,177 ETH	
3	Tether USDT Buy	$1.00	▲0.04%	▼0.04%	$62,499,718,041	$64,376,151,026 64,329,603,115 USDT	62,454,526,907 USDT	
4	Binance Coin BNB Buy	$312.58	▲9.04%	▲35.99%	$48,145,422,368	$1,962,717,211 6,254,912 BNB	153,432,897 BNB	
5	Cardano ADA	$1.41	▲7.23%	▲39.24%	$45,002,839,114	$2,725,935,851 1,935,069,948 ADA	31,946,328,269 ADA	
6	Dogecoin DOGE Buy	$0.2716	▲7.56%	▲62.46%	$35,629,948,823	$2,116,279,315 7,735,056,081 DOGE	130,228,392,047 DOGE	
7	XRP XRP	$0.7226	▲14.88%	▲39.75%	$33,309,358,526	$3,151,986,174 4,366,775,115 XRP	46,146,927,647 XRP	
8	USD Coin USDC	$1.00	▲0.02%	▼0.05%	$25,387,739,431	$2,374,343,302 2,373,317,365 USDC	25,376,769,571 USDC	

Coin Market Cap – Jun 29, 2021

Ethereum (ETH)

Ethereum ဟာ Bitcoin ပြီးရင် ဒုတိယမြောက် အရေးအကြီးဆုံး Cryptocurrency ဖြစ်ပါတယ်။ လက်ရှိလည်း Market Cap ဒေါ်လာ (၂၅၉) ဘီလီယံကျော်နဲ့ ဒုတိယနေရာမှာ ရှိနေပါတယ်။ တီထွင်ဆန်းသစ်မှု အသစ်တွေနဲ့ ကြီးမားတဲ့ရည်မှန်းချက်တွေရှိပြီး Cryptocurrency တစ်ခု ဆိုတာထက် အများကြီးပိုတဲ့ နည်းပညာတစ်ခုပါ။

Ethereum အကြောင်း ပြောစရာတွေ များလို့ တစ်ကယ်တော့ နောက်တစ်ခန်း သပ်သပ်ခွဲပြီး ပြောရမှာပါ။ ဒါပေမယ့် Ethereum အကြောင်း မပြောဘဲ တချို့ Altcoin တွေအကြောင်းပြောလို့ မရတဲ့အတွက် အခန်းမခွဲတော့ဘဲ ဒီနေရာမှာပဲ တစ်ခါထဲ ထည့်ပြောပါတော့မယ်။

Ethereum က Blockchain နည်းပညာဖြစ်ပြီး အဲ့ဒီနည်းပညာကို အသုံးပြုထားတဲ့ Ether ကမှ တစ်ကယ့် ငွေကြေးကဲ့သို့ အသုံးပြုနိုင်သော Cryptocurrency လို့ ပြောမှ ပိုတိကျပါမယ်။ ဒီလိုမျိုး နည်းပညာနဲ့ ငွေကြေး၊ နှစ်မျိုးကွဲပေမယ့် ပြောရတာလွယ်အောင် Ethereum လို့ တစ်မျိုးထဲပဲ ပေါင်းပြီး ဆက်ပြောသွားပါမယ်။

Ethereum ကို Vitalik Buterin လို့ခေါ်တဲ့ ရုရှား–ကနေဒီယန် ပရိုဂရမ်မာတစ်ဦးက စတင်အဆိုပြုခဲ့ပြီး White Paper ကိုလည်း သူကိုယ်တိုင်ပဲ ရေးသားခဲ့လို့ Ethereum ရဲ့ တည်ထောင်သူလို့ သိရှိထားကြပါတယ်။ တစ်ကယ်တော့ Ethereum ကို စတင်တည်ထောင်သူထဲမှာ ပါဝင်တယ်လို့ ပြောလို့ရတဲ့ တစ်ခြား ပညာရှင် (၄) ဦးလည်း ရှိပါသေးတယ်။ ဒီလူတွေထဲက တချို့အကြောင်းကို နောက်ပိုင်းမှာ ဆက်ပြောစရာရှိပါတယ်။

Ethereum ကတော့ Litecoin တို့ Dogecoin တို့လို Bitcoin Source Code ကနေ ဆင်းသက်လာတာ မဟုတ်တော့ပါဘူး။ သူ့ကိုယ်ပိုင် Blockchain နည်းပညာနဲ့ဖြစ်သွားပါပြီ။ Proof of Work အပါအဝင် အခြေခံအားဖြင့် Bitcoin နဲ့ သဘောသဘာဝ ဆင်တူပါတယ်။ မတူကွဲပြားတာတွေလည်း ရှိပါတယ်။ ဥပမာ – Bitcoin က Transaction တွေကိုသာ Blockchain ထဲမှာသိမ်းပြီး Balance ကို မသိမ်းပါဘူး။ Ethereum ကတော့ Balance ကိုပါ ထည့်သိမ်းပါတယ်။

Vitalik Buterin

နောက်တစ်ခုအနေနဲ့ Bitcoin က ကွိုင်အရေအတွက် (၂၁) သန်းမှာ Max Supply ကို သတ်မှတ်ထားပေမယ့် Ethereum မှာ Max Supply မရှိပါဘူး။ ဒါပေမယ့် တစ်နှစ်အတွင်း အမြင့်ဆုံးပမာဏ Annual Max Supply အနေနဲ့ ကွိုင် (၁၈) သန်းလို့ သတ်မှတ်ထားပါတယ်။

Ethereum က Block တွေ Hash လုပ်ဖို့အတွက် Ethash လို့ခေါ်တဲ့ Algorithm ကို အသုံးပြုပါတယ်။ ဒီ Algorithm ရဲ့ ထူးခြားချက်ကတော့ Block ၃၀,၀၀၀ ပြည့်တိုင်း DAG လို့ခေါ်တဲ့ Data Set တစ်ခုကို ဖန်တီးပါတယ်။ Blockchain ရဲ့ Size ကြီးလာတာနဲ့အမျှ DAG ရဲ့ Size လည်း လိုက်ကြီးလာမှာဖြစ်ပြီး လက်ရှိ 3.5 GB ရှိပါတယ်။ Ethereum အတွက် Mine လုပ်လိုသူဟာ အဲ့ဒီ Data Set ကို ရယူထားဖို့ လိုအပ်ပါတယ်။ Hash လုပ်တဲ့အခါ အဲ့ဒီ Data Set ထဲက အစိတ်အပိုင်းကို ယူပြီး ထည့်လုပ်ရတာပါ။ ဒါကြောင့် Ethereum Block အတွက် Hash လုပ်ဖို့ဆိုရင် Processing Power ကောင်းယုံနဲ့ မရဘဲ၊ Memory လည်း များများရှိဖို့လည်း လိုပါတယ်။ Memory I/O မြန်ဖို့လည်း လိုပါတယ်။ ဘာကြောင့်ဒီ ဒီဇိုင်းကိုသုံးရသလဲဆိုတော့ Ethereum ကို ASIC စက်တွေနဲ့ Mine လုပ်လို့ မရစေဖို့အတွက်ပါ။ သာမန်လူတွေက သာမန် GPU ရှိယုံနဲ့ Mine လုပ်စေနိုင်ဖို့ Chance ကို ပိုပေးထားလိုက်တဲ့ သဘောပဲ ဖြစ်ပါတယ်။ ဒါဟာလည်း မှတ်သားစရာ အချက်တစ်ခုပါ။

Smart Contract

Ethereum ရဲ့ တီထွင်မှုတွေထဲမှာ အရေးအကြီးဆုံးကတော့ Smart Contract လို့ခေါ်တဲ့ လုပ်ဆောင်ချက်ပါ။ Smart Contract ဆိုတာ သတ်မှတ်ချက်တွေနဲ့ ပြည့်စုံတဲ့အခါ အလိုအလျောက် လုပ်ရမယ့် လုပ်ဆောင်ချက်တွေကို ပရိုဂရမ်ကုဒ်ကဲ့သို့ ရေးသားပြီး Blockchain ထဲမှာ သိမ်းဆည်းနိုင်ခြင်း ဖြစ်ပါတယ်။

ဥပမာ – ကြိုတင်ငွေပေးချေပြီး မှာယူတဲ့သူ အယောက် (၂၀) ရှိရင် ကိတ်မုန့်လုပ်ပြီး ရောင်းချင်တယ်။ အယောက် (၂၀) မပြည့်ရင်တော့ မရောင်းချင်ဘူး။ ဒါကို ကြေညာပြီး အမှာစာတွေလက်ခံတဲ့အခါ ကြိုတင်ငွေပေးချေမှု (၁၅) ခုရခဲ့ပေမယ့် (၂၀) မပြည့်လိုက်ဘူး ဆိုပါစို့။ ဒါကြောင့် မရောင်းနိုင်တော့တဲ့အတွက် ငွေပေးချေထားသူ (၁၅) ယောက်ကို တစ်ယောက်ချင်း ငွေပြန်လွှဲ ပေးရတော့မှာပါ။

ဒီလိုကိစ္စမျိုးမှာ Smart Contract နဲ့ အယောက် (၂၀) ပြည့်မှသာ အပြီးသတ် လက်ခံဖို့နဲ့ မပြည့်ခဲ့ရင် ပြန်လွှဲပေးဖို့ ကြိုတင်သတ်မှတ်ထားလိုက်မယ်ဆိုရင် ကိုယ့်ဘာသာ တစ်ယောက်ချင်းပြန်လွှဲပေးနေစရာ မလိုတော့ပါဘူး။ သတ်မှတ် Condition နဲ့အညီ Smart Contract က အလိုအလျောက် လုပ်ပေးသွားမှာပါ။

ဒါဟာ အလွန်အရေးပါတဲ့ တီထွင်မှုဖြစ်ပါတယ်။ ဒီတီထွင်မှုကြောင့် Blockchain ကို ငွေပေးငွေယူ Transaction အတွက်သာမက တစ်ခြား ငွေကြေးဝန်ဆောင်မှု လုပ်ငန်းတွေအတွက်ပါ အသုံးပြုလို့ ရသွားနိုင်မှာပါ။ ဥပမာ – ငွေစုတာကိုလက်ခံပြီး သုံးလပြန်မထုတ်ဘဲစုထားရင် အတိုး (၂%) ပေးမယ်၊ မပြည့်ခင် ပြန်ထုတ်ရင်တော့ မပေးဘူးဆိုတာမျိုးကို Smart Contract နဲ့ သတ်မှတ်ထားလိုက်လို့ရနိုင်ပါတယ်။ ဒီနည်းနဲ့ ဗဟိုထိမ်းချုပ်မှု မလိုတဲ့ ငွေစုငွေချေးလုပ်ငန်း၊ ရင်းနှီးမြှုပ်နှံမှုလုပ်ငန်း၊ ငွေလဲလုပ်ငန်း၊ အာမခံလုပ်ငန်းတို့လို ငွေကြေးဝန်ဆောင်မှုတွေ လုပ်လို့ရသွားနိုင်မှာပါ။ ဒီသဘောသဘာဝကို Decentralized Finance (DeFi) လို့ခေါ်ပါတယ်။

Smart Contract နည်းပညာကို အခြေခံပြီး ဗဟိုမဲ့ အသုံးချဆော့ဖ်ဝဲတွေလည်း တီထွင်လို့ ရနိုင်ပါသေးတယ်။ Decentralized Application (Dapps) လို့ ခေါ်ပါတယ်။ App က Blockchain ထဲမှာ ရှိနေတာဖြစ်လို့ Server လို ဗဟိုစနစ်တွေ မလိုအပ်တော့တာပါ။ ဒီလိုမျိုး တီထွင်ဆန်းသစ်မှုတွေကြောင့် Ethereum က Cryptocurrency ကဏ္ဍကို တစ်ခေတ်ဆန်း သွားစေတယ်လို့ဆိုရမှာပါ။

Ethereum Ecosystem

ERC-20

Ethereum အတွက် Ethereum Improvement Proposal (EIP) နဲ့ Ethereum Request for Comment (ERC) လို့ခေါ်တဲ့ လုပ်ငန်းစဉ်တွေ ရှိပါတယ်။ လိုရင်းကတော့ Ethereum နည်းပညာမှာ ဖြည့်စွက်မှုတွေ ပြုလုပ်လိုရင် Proposal စာတမ်းတင်ရတဲ့ သဘောပါ။ အဲ့ဒီစာတမ်းပေါ်မှာ အများက ဝိုင်းဝန်းဆွေးနွေးပြီး အတည်ပြုလိုက်တဲ့အခါ ထပ်တိုးနည်းပညာအနေနဲ့ ပါဝင်သွားတာပါ။ အဲ့ဒီထပ်တိုးနည်းပညာတွေထဲမှာ အရေးပါတဲ့တစ်ခုကတော့ ERC-20 ပဲ ဖြစ်ပါတယ်။ ဒါဟာ Ethereum Blockchain ကို အသုံးပြုပြီး ကိုယ်ပိုင် Cryptocurrency Token တွေ ဖန်တီးလို့ရတဲ့ နည်းပညာတစ်ခုပါ။

ဥပမာ – စာဖတ်သူက BakeCoin (BAKE) လို့ခေါ်တဲ့ ကိုယ်ပိုင် Cryptocurrency တစ်မျိုးကို တီထွင်ချင်တယ်၊ ပြီးတော့ မုန့်ဆိုင်တစ်ဆိုင် ဖွင့်ပြီး အဲ့ဒီမုန့်ဆိုင်ကနေ မုန့်မှာစားချင်ရင် BakeCoin နဲ့ဝယ်စားရမယ်လို့ သတ်မှတ်ထားချင်တယ်ဆိုပါစို့။

ဒါဆိုရင်ပထမဆုံး BakeCoin ကိုဖန်တီးဖို့အတွက် ERC-20 သတ်မှတ်ချက်နဲ့အညီ Smart Contract တစ်ခုကို ဖန်တီးရပါမယ်။ ဘယ်လိုဖန်တီးရမလဲဆိုတဲ့ နည်းပညာတော့ ထည့်မပြောနိုင်ပါဘူး။ ကွန်ပျူတာ

Programming တွေ ပါလာပြီမို့လို့ပါ။ ကုဒ်တွေကိုယ်တိုင်ရေးစရာ မလိုဘဲ Auto Generate လုပ်ပေးနိုင်တဲ့ နည်းပညာတွေလည်း ရှိတော့ ရှိနိုင်ပါတယ်။ ဒီနေရာမှာတော့ Smart Contract တစ်ခုကို ERC-20 က သတ်မှတ်ထားတဲ့အတိုင်း ဖန်တီးလိုက်ပြီလို့ပဲ သဘောထားပါ။

Smart Contract မှာ သတ်မှတ်ထားတာက စာဖတ်သူရဲ့ Ethereum Wallet Address ကို 1 ETH ပို့ရင် BAKE Token (၁၀) ခု ပြန်ပေးပါမယ်။ စာဖတ်သူရဲ့မုန့်ဆိုင်မှာ မုန့်တစ်ခုကို 1 BAKE နဲ့ ရောင်းတယ်ဆိုရင် အဲ့ဒီလူက မုန့် (၁၀) ခု ဝယ်စားလို့ရသွားပါပြီ။ တစ်ခြားလူတစ်ယောက်က စာဖတ်သူရဲ့ မုန့်ဆိုင်မှာ ဝယ်စားချင်ပေမယ့် BAKE မရှိပါဘူး။ ဒါကြောင့် ရှိတဲ့သူဆီက BAKE Token တစ်ခုကို 10 USD နဲ့ ဝယ်ယူလိုက်မယ်ဆိုရင် 1 BAKE = 10 USD တန်သွားတဲ့ သဘောပါပဲ။

ERC-20 Token တွေဟာ Native Coin မဟုတ်လို့ Mine တူးပြီး ရှာယူလို့တော့ မရပါဘူး။ မူလဖန်တီးရှင်ရဲ့ Smart Contract ပါ အချက်အလက်များနဲ့ အညီသာ ရယူနိုင်မှာပါ။ ငွေပေးငွေယူ လုပ်တာကတော့ Ethereum Blockchain ပေါ်မှာ ETH ကို အပေးအယူ လုပ်သလိုပဲ လုပ်သွားတာပါ။ Wallet အနေနဲ့ Ethereum Wallet ကိုပဲ အသုံးပြုနိုင်ပါတယ်။ ပင်မ Transaction မှာ 0 ETH ကို ပို့ပြီး အဲ့ဒီ Transaction ထဲမှာ Token Transaction ကို တွဲထည့်ရတဲ့ သဘောမျိုးပါ။ ETH ကို ထည့်လွှဲစရာမလိုဘဲ Token Transaction ပြုလုပ်ဖို့အတွက်လွှဲခ ကိုတော့ ETH နဲ့ ပေးရပါလိမ့်မယ်။ Ethereum မှာ ဒီလိုအဖိုးအခမျိုးကို Gas Fee လို့ခေါ်ပါတယ်။

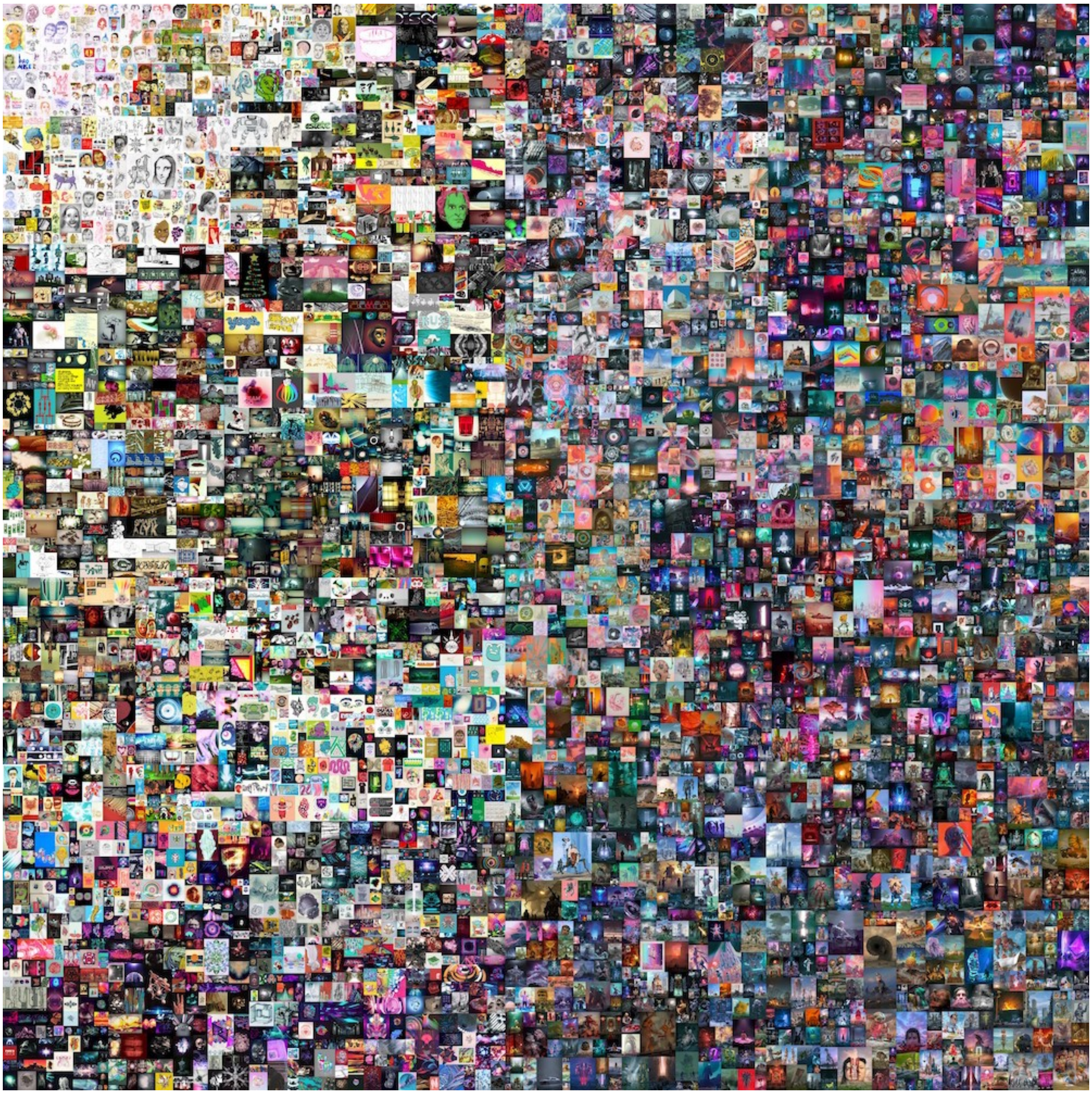
ဒီနည်းနဲ့ ကိုယ်ပိုင် Cryptocurrency Token တွေကို Ethereum Blockchain ထဲမှာပဲ ဖန်တီးအသုံးပြုနိုင်ပါတယ်။ ဒီနည်းနဲ့ပဲ ဖန်တီးထားတဲ့ အထင်ကရ Cryptocurrency တွေလည်း အများကြီး ရှိနေပါတယ်။

ERC-721 (NFT)

နောက်ထပ်အရေးပါတဲ့ သဘောသဘာဝဖြစ်တဲ့ ERC-721 ဆိုတာကတော့ အခုနောက်ပိုင်း ခေတ်စားနေတဲ့ NFT ခေါ် Non-Fungible Token တွေ ဖန်တီးဖို့အတွက် အသုံးပြုရတဲ့ နည်းပညာ ဖြစ်ပါတယ်။

The First 5000 Days လို့ခေါ်တဲ့ ဒစ်ဂျစ်တယ် Art တစ်ခုဟာ NFT Token တစ်ခုအနေနဲ့ လေလံပစ်ရောင်းချရာမှာ ဒေါ်လာ (၆၉) သန်း ရခဲ့ပါတယ်။ ဒီလို အင်တာနက်မှာ လူတိုင်းကြည့်လို့ရ၊ Download လုပ်ယူလို့ရတဲ့ ပုံတစ်ပုံကို ဒီလောက်ထိ ငွေပေးဝယ်ကြတာ ဘာသဘောလဲဆိုပြီးတော့ နားမလည်နိုင်စရာပါ။ ပို

ပြီးတော့ နားလည်ရခက်သွားတာက ပုံကိုဝယ်တာလည်း မဟုတ်ပါဘူး။ အဲ့ဒီပုံရဲ့ Token ကို ဝယ်လိုက်တာပါ။ တစ်ကယ့်ကို ခေါင်းရှုပ်စရာ ဖြစ်နေတော့တာပါပဲ။



The First 5000 Days

စာရေးသူကတော့ ဒီလိုနားလည်မိပါတယ်။ ပြတိုက်မှာ ပြထားတဲ့ ရှားပါး ပန်းချီကားတစ်ချပ် ဆိုကြပါစို့။ အဲ့ဒီပန်းချီကားကို ပိုင်ဆိုင်လိုရင် ဒေါ်လာ (၁၀) သန်းပေးရမယ်လို့ သတ်မှတ်ထားရင် လိုချင်တဲ့သူက ဒေါ်လာ (၁၀) သန်းပေး ဝယ်ရပါတယ်။ ဒီလိုပေးလိုက်တဲ့အခါ ပြတိုက်က ပန်းချီကားရဲ့ ပိုင်ရှင်ဖြစ်ကြောင်း

Certificate ထုတ်ပေးလိုက်လို့ သူက အဲ့ဒီပန်းချီကားရဲ့ ပိုင်ရှင်ဖြစ်သွားပါပြီ။ ဒါပေမယ့် ပန်းချီကားကို အိမ်ကို ယူသွားလို့ မရပါဘူး။ ပြတိုက်မှာပဲ ထားရပါတယ်။ သူတစ်ယောက်ထဲ ကြည့်လို့ရတာလည်း မဟုတ်ပါဘူး။ မည်သူမဆို ပြတိုက်မှာ လာကြည့်လို့ရပါတယ်။ ဒါပေမယ့် တစ်ကယ့် ပိုင်ရှင်ကတော့ သူပါပဲ။ ဘာကြောင့်လဲဆိုတော့ သူ့နာမည်နဲ့ သူသာလျှင် ပိုင်ရှင်ဖြစ်ကြောင်း ပြတိုက်က ထုတ်ပေးထားတဲ့ Certificate ရှိနေလို့ပါ။ ဒီသဘောပါပဲ။

ဒါက နည်းပညာနဲ့တော့ တိုက်ရိုက် မဆိုင်ပါဘူး။ ဘာကြောင့်များ လူတိုင်း အင်တာနက်မှာ Download လုပ်လို့ ရနေတဲ့ ဒစ်ဂျစ်တယ် Art တစ်ခုရဲ့ Token ကို ဒေါ်လာသန်းပေါင်းများစွာ ပေးရတာလည်းဆိုတာကို နားလည်အောင် ကြိုးစားကြည့်တာပါ။ Token ပိုင်ရှင်ဟာ အဲ့ဒီ Original Art ရဲ့ ပိုင်ရှင်ဖြစ်ကြောင်း အာမခံချက်တစ်ခု ဖြစ်နေလို့ပါ။ NFT Token ဟာ ပြတိုက်ကထုတ်ပေးတဲ့ Certificate နဲ့တူပါတယ်။ နှစ်ခု မရှိပါဘူး။ အတုလုပ်လို့ မရပါဘူး။ Certificate ထဲမှာ ပိုင်ရှင်ဘယ်သူဘယ်ဝါဆိုတာ ပါနေပါတယ်။

NFT Token တွေကို ERC-721 ပါ သတ်မှတ်ချက်များနဲ့အညီ Ethereum Blockchain ထဲမှာ မည်သူမဆို ဖန်တီးလို့ရပါတယ်။ ဒစ်ဂျစ်တယ် Art တွေကို NFT အနေနဲ့ နားလည်ရတာ ခက်နိုင်ပေမယ့် ကားတစ်စီးလို အရာမျိုး ဆိုရင်တော့ နားလည်ရ နည်းနည်း ပိုလွယ်နိုင်ပါတယ်။

ဥပမာ – Owner Book လက်ဝယ်ရှိသူကို ကားတစ်စီးရဲ့ ပိုင်ရှင်လို့ အကြမ်းဖျင်း သတ်မှတ်ကြပါတယ်။ ဒါပေမယ့် လက်တွေ့မှာ Owner Book ကို ခိုးယူလာတာလည်း ဖြစ်နိုင်တယ်၊ အတုလုပ်ထားတာလည်း ဖြစ်နိုင်ပါတယ်။ ဒါကြောင့် ကားနံပါတ်၊ အမျိုးအစား၊ အင်ဂျင်နံပါတ် စတဲ့အချက်အလက်တွေနဲ့အတူ ပိုင်ရှင်ရဲ့ အချက်အလက်တွေ ပါဝင်တဲ့ ERC-721 Token တစ်ခုကို ဖန်တီးလိုက်ရင်တော့ အဲ့ဒီ Token ကို အတုလုပ်လို့ မရတော့ပါဘူး၊ ခိုးယူလို့လည်း မရနိုင်ပါဘူး။

Token ထဲမှာ Owner ရဲ့ Wallet Address ပါဝင်လို့ တစ်ကယ့်ပိုင်ရှင် အစစ်ကသာ Verify လုပ်နိုင်မှာပါ။ Token ကို အရောင်းအဝယ် လုပ်တယ်ဆိုတာ Token ထုတ်ထားတဲ့ ကားရဲ့ပိုင်ရှင် အစစ်အမှန်ဘယ်သူလဲဆိုတာကို အရောင်းအဝယ် လုပ်လိုက်တာပါပဲ။ အရောင်းအဝယ် ပြုလုပ်လိုတဲ့အခါ ဝယ်ယူသူရဲ့ Address ထံ Token ကို ပို့ပေးလိုက်ယုံပါပဲ။ Smart Contract က Token ထဲက Owner Address ကို ပိုင်ရှင်အသစ်ရဲ့ Address နဲ့ အလိုအလျှောက် Update လုပ်ပြီး Blockchain ထဲမှာ ထပ်ထည့်ပေးလိုက်မှာပဲ ဖြစ်ပါတယ်။ ဒါကြောင့် လက်ရှိပိုင်ရှင်ဟာ လွှဲပြောင်းဝယ်ယူလိုက်သူ ဖြစ်သွားပါပြီ။

ERC-20 Token တွေဟာ ငွေကြေးတစ်ရပ်ကဲ့သို့ အလဲအလှယ် လုပ်လို့ရပါတယ်။ ကိုယ့်အိတ်ထဲက ၅၀၀၀ တန်တစ်ရွက်နဲ့ သူများအိတ်ထဲက ၅၀၀၀ တန်တစ်ရွက် တန်ဖိုးချင်းအတူတူပါပဲ။ အသုံးပြုတဲ့အခါ လက်ခံသူက သူ့ ၅၀၀၀ ပဲ ဖြစ်ဖြစ် ကိုယ့် ၅၀၀၀ ပဲဖြစ်ဖြစ် အတူတူပဲ လက်ခံမှာပါ။ ဒီသဘောမျိုးကို Fungible ဖြစ်တယ်လို့ ဆိုတာပါ။ ERC-721 Token တွေကတော့ သက်ဆိုင်ရာ Property တစ်ခုအတွက် ထုတ်ယူထားတဲ့ Unique Token တွေဖြစ်လို့ Fungible မဖြစ်ပါဘူး။ Token ချင်းဆင်တူပေမယ့် ကားတစ်စီးရဲ့ Token နဲ့ အိမ်တစ်လုံးရဲ့ Token တန်ဖိုးချင်းမတူသလို အလဲအလှယ်လည်း လုပ်လို့ရမှာ မဟုတ်ပါဘူး။ ဒါကြောင့် Non-Fungible Token (NFT) လို့ ခေါ်ကြတာပါ။

ဒါကြောင့် ERC-721 ခေါ် NFT Token ဆိုတာ၊ ဒစ်ဂျစ်တယ် Property တွေ ရုပ်ဝတ္ထုပစ္စည်းတွေ အတွက် Unique ဖြစ်တဲ့၊ နှစ်ခုမရှိတဲ့၊ အတုလုပ်လို့မရနိုင်တဲ့ Token ထုတ်ယူပြီး အဲ့ဒီ Token ကို လက်ဝယ်ထားခြင်းဖြင့် ပိုင်ရှင်အစစ်အမှန်ဖြစ်ကြောင်း အတည်ပြုနိုင်တဲ့ နည်းပညာ လို့ ဆိုနိုင်ပါတယ်။။

ETH vs. ETC

Ethereum Smart Contract ကို အသုံးပြုပြီး ဖန်တီးထားတဲ့ The DAO လို့ခေါ်တဲ့ လုပ်ငန်းတစ်ခု ရှိပါတယ်။ ဝန်ထမ်းတစ်ဦးမှ မရှိဘဲ Smart Contract နဲ့ Automate လုပ်ထားတဲ့ ရင်းနှီးမြှုပ်နှံမှု လုပ်ငန်းပါ။ ရင်းနှီးမြှုပ်နှံလိုသူတွေက DAO Token တွေ ဝယ်ရပါတယ်။ Project Proposal လက်ခံရရှိတဲ့အခါ Token လက်ဝယ်ရှိသူတွေက Vote လုပ်ပြီး အဲ့ဒီပရောဂျက်အတွက် အရင်းအနှီး ထုတ်ပေးမပေး ဆုံးဖြတ်ရတာပါ။ အိုင်ဒီယာကောင်းပေမယ့်လည်း The DAO ရဲ့ အားနည်းချက် တစ်ခုကြောင့် (၂၀၁၆) ခုနှစ်မှာ Ethereum Network ကို အဟက်ခံရပြီး ဒေါ်လာသန်း (၅၀) လောက် တန်ကြေးရှိတဲ့ DAO Token တွေ ခိုးယူခံလိုက်ရပါတယ်။

တချို့က ဟက်ခံရတဲ့အခြေအနေ မရောက်ခင် အနေအထားကနေ စပြီး Blockchain ကို အသစ်ခွဲထုတ်လိုက်စေချင်ကြပါတယ်။ ဒီလိုခွဲထုတ်လိုက်ခြင်းအားဖြင့် ဟက်ခံရတဲ့ Block တွေမပါတဲ့ Blockchain အသစ်တစ်ခုနဲ့ ဆုံးရှုံးနစ်နာမှုတွေ မရှိတော့ဘဲ ရှေ့ဆက်သွားလိုက်စေချင်တဲ့ သဘောပါ။ တချို့ကတော့ လက်ရှိအတိုင်းပဲ ဆက်သွားစေချင်ပါတယ်။ ငွေကြေးစနစ်ဆိုတာ ဒီလိုပဲ ပြဿနာတွေ ကြုံရတတ်တယ်။ နောက်မဖြစ်အောင်ပြင်ပြီး အရှိအတိုင်းပဲလက်ခံရမယ်။ ပြဿနာကြုံတိုင်း ကိုယ့်သဘောနဲ့ကိုယ် ပြန်ပြင်ကြမယ်ဆိုရင် စစ်မှန်တဲ့အရာ မဟုတ်တော့ဘူးလို့ သဘောထားကြပါတယ်။

မဲခွဲလိုက်တဲ့အခါ ရလဒ်အရ Blockchain အသစ်တစ်ခု ခွဲထုတ်လိုက်ကြပါတယ်။ ဒါပေမယ့် တချို့က ဒါကို လက်မခံဘဲ မူလလက်ဟောင်း Blockchain ကိုပဲ ဆက်လက် အသုံးပြုခဲ့ကြပါတယ်။ ဒါကြောင့် လက်ရှိမှာ Ethereum ဟာ **Ethereum** (ETH) နဲ့ **Ethereum Classic** (ETC) ဆိုပြီး နှစ်မျိုးကွဲနေပါတယ်။ နှစ်မျိုးလုံး အခုထိ ဆက်လက်တည်ရှိနေပါတယ်။ ၂၀၂၀ ခုနှစ်ထဲမှာ ETC ဈေးတွေ တက်နေလို့ လေ့လာကြည့်လိုက်တဲ့ အခါ Ethereum ကို စိတ်ဝင်စားလို့ ဝယ်ယူလိုသူတွေက ETH ဝယ်ရမယ့်အစား မှားပြီး ETC ကို ဝယ်နေကြ လို့ ဆိုတာကို တွေ့ခဲ့ကြရပါတယ်။ ဘယ်လိုပဲဖြစ်ဖြစ် ETC ဟာလည်း လက်ရှိ အဓိက Cryptocurrency အနေနဲ့ ဆက်လက်တည်ရှိနေဆဲ ဖြစ်ပါတယ်။

Proof of Stake

Ethereum ဟာလည်း Bitcoin လိုပါပဲ၊ Scalability ပြဿနာရှိပါတယ်။ တစ်စက္ကန့်ကို Transaction (၁၅) ခုခန့်သာ ပြုလုပ်နိုင်လို့ Bitcoin ထက်တော့ သာသွားပေမယ့် Visa ရဲ့ တစ်စက္ကန့် (၂,၀၀၀) ဆိုတာနဲ့ယှဉ် ရင် အများကြီး လိုအပ်ပါသေးတယ်။ ဒီပြဿနာကို ဖြေရှင်းမယ့် နည်းပညာတွေနဲ့အတူ Ethereum 2.0 ခေါ် Version အသစ်တစ်ခု မကြာခင်မှာ လာဖို့ရှိနေပါတယ်။ သူ့ရဲ့ ဖြစ်စွက်ချက်တွေထဲမှာ Proof of Stake လုပ်ဆောင်ချက်လည်း ပါဝင်ပါတယ်။

Bitcoin တို့ Ethereum တို့ဟာ Proof of Work လို့ခေါ်တဲ့ သဘောသဘာဝကို လက်ရှိအသုံးပြုထားကြပါ တယ်။ Proof of Work အကြောင်းကို ရှေ့ပိုင်းမှာ ဖော်ပြခဲ့ပြီး ဖြစ်ပါတယ်။ ဒီ Proof of Work ကြောင့်ပဲ လျှပ်စစ်စွမ်းအင် အသုံးပြုမှု များပြားတဲ့ပြဿနာရှိနေပြီး Block အသစ်တွေကို အချိန်အကန့်အသတ်နဲ့သာ ထည့်သွင်းနိုင်လို့ Transaction အရေအတွက် နည်းနေတာပါ။ ဒါကြောင့် Proof of Work ကို အစားထိုးနိုင် မယ့် နည်းလမ်းတွေ ကြံဆကြရာမှာ Proof of Stake က ရေပန်းအစားဆုံး ဖြစ်နေတာပါ။ သူ့ရဲ့အလုပ်လုပ် ပုံက ဒီလိုပါ။

၁။ Mine တူးလိုသူဟာ သတ်မှတ်ကွိုင်ပမာဏကို Stake လုပ်ပြီး Network ထဲမှာ ကြိုအပ်ထားရပါတယ်။

၂။ အဲ့ဒီလိုကြိုအပ်ထားတဲ့ Node တွေထဲက ကျပမ်း Random ရွေးပြီး Block အသစ်ထည့်ခွင့်ပေးပါတယ်။

၃။ လုပ်စရာရှိတဲ့ Transaction တွေကို Verify လုပ် စစ်ဆေးခြင်းတွေ သေချာလုပ်ပြီး Block အသစ်ကို ထည့်ပေးလိုက်ရင် ဆုငွေကိုရပါတယ်။

၄။ မမှန်မကန်ထည့်ခဲ့ရင် အပ်ထားတဲ့ ကွိုင်ထဲကနေ ဒါဏ်ကြေးပြန်ဖြတ်ပါတယ်။ ဒါကြောင့် ကြိုအပ်ရတဲ့ ကွိုင်က ရမယ့်ဆုငွေထက် များတဲ့ပမာဏ ဖြစ်ပါလိမ့်မယ်။

၅။ အလှည့်များများရချင်ရင် များများအပ်ထားနိုင်ပါတယ်။ ဥပမာ – 10 ETH အပ်ထားတဲ့သူက Chance ၁၀ ခုရပြီး 5 ETH အပ်ထားတဲ့သူက Chance ၅ ခုရမယ်ဆိုရင် Random ရွေးတယ်ဆိုပေမယ့် 10 ETH အပ်ထားတဲ့သူက ပိုအလှည့် ရမှာပါ။ ဒီလို ပိုအပ်ရင် ပိုအလှည့်ရတယ်ဆိုပြီး မတရားသဖြင့် အများအပြား အပ်ထားလို့လည်း သူချည်းပဲ အလှည့်ရမှာတော့ မဟုတ်ပါဘူး။ တစ်ခြားသူတွေမှာလည်း သင့်တင့်တဲ့ Chance ရှိနေအောင် တွက်ချက်တဲ့ Algorithm တွေ ရှိပါတယ်။

ဒီနည်းနဲ့ Mine တူးဖို့အတွက် Hash ကိုရှာရတာ မဟုတ်တော့ပဲ အပ်ငွေပေါ်မူတည်ပြီး အလုပ်လုပ်တာ ဖြစ်သွားလို့ စွမ်းအင်လည်း အလွန်အကျွံသုံးစရာ မလိုတော့ပါဘူး။ အချိန်လည်း စောင့်စရာမလိုတော့ဘဲ ချက်ခြင်း ထည့်သွင်းနိုင်မှာဖြစ်လို့ Transaction လည်း အရမ်းမြန်သွားပါပြီ။

ဒီ Proof of Stake နည်းစနစ်ကို အသုံးပြုနေတဲ့ Cryptocurrency တွေ အခုလည်း ရှိနေပြီး ဖြစ်ပါတယ်။ တချို့ Proof of Storage တို့ Proof of Authority တို့ Proof of History တို့လို နည်းစနစ်တွေကို အသုံးပြုထားတဲ့ Cryptocurrency တွေလည်း ရှိနေပါသေးတယ်။

Proof of Stake မှာလည်း အားနည်းချက်တချို့တော့ ရှိပါတယ်။ အမြင်သာဆုံးကတော့ အခုမှစမယ့် Cryptocurrency တစ်ခုဟာ Proof of Stake နည်းစနစ်ကို အသုံးပြုချင်ရင် Pre-Mine လုပ်ပြီး ကွိုင်တွေ ကြိုထုတ်ထားမှပဲ ရပါတော့မယ်။ ဒီတော့မှ အများဝိုင်းပြီး Mine မတူးခင် Stake လုပ်ပြီး အပ်စရာ ကွိုင်တွေ ကြိုရှိနေမှာပါ။ Fair Launch ခေါ် မူလ တီထွင်သူက ကွိုင်တွေကို ကိုယ့်အတွက် ကြိုထုတ်မယူထားပဲ သွားတဲ့ နည်းကို အသုံးပြုလို့ မရနိုင်တော့ပါဘူး။

နောက်ပြဿနာတစ်ခုက Mine တူးချင်တဲ့အတွက် ကွိုင်တွေကို အပ်ထားကြသူ များလာလို ငွေကြေး လည်ပါတ်မှု Circulation နည်းသွားမှာကိုလည်း စိတ်ပူရပါတယ်။ ပြီးတော့ မရိုးသားတဲ့သဘောနဲ့ တမင် ရည်ရွယ်တာ မဟုတ်ပေမယ့် Block ထည့်ဖို့ ကိုယ့်အလှည့်ရချိန်မှာ အင်တာနက်ကြောင့်ပဲဖြစ်ဖြစ် ကိုယ့်စက် Node ပြဿနာကြောင့်ပဲဖြစ်ဖြစ် မထည့်ပေးနိုင်တဲ့အခါမျိုးမှာ ဒါဏ်ကြေးအနေနဲ့ အပ်ထားတဲ့ကွိုင်ထဲက အဖြတ်ခံရမှာကိုလည်း တချို့က မလိုလားကြပါဘူး။ ဒါကြောင့် အခုဒီစာရေးနေချိန်ထိ လက်ရှိ Proof

of Stake ကို အသုံးပြုထားတဲ့ Cryptocurrency တွေမှာ ဒါဏ်ရိုက်တဲ့အလုပ်ကို မူအားဖြင့်သာ သတ်မှတ်ထားပြီး တစ်ကယ်လက်တွေ့ မလုပ်ကြသေးပါဘူး။

ပြီးတော့ Proof of Work မှာလို ခက်ခက်ခဲခဲ ရင်းနှီးမြှုပ်နှံပြီး လုပ်ဖို့မလိုဘဲ ကွိုင်ရှိသူ မည်သူမဆို ဝင်လုပ်လို့ ရနေတာကိုလည်း လုံခြုံရေးအတွက် တချို့က စိတ်ပူကြပါတယ်။ ဒါကြောင့် Proof of Work နဲ့ Proof of Stake ကို တွဲသုံးကြတာတွေလည်း ရှိပါတယ်။ Proof of Stake ဟာ အလားအလာကောင်းပေမယ့် ဖြေရှင်းစရာအခက်အခဲတွေ ရှိနေပြီး စောင့်ကြည့်ဖို့ လိုအပ်နေသေးတဲ့ နည်းစနစ်လို့ ဆိုနိုင်ပါတယ်။

Proof of Work မှာ 51% Attack နဲ့ ဒုက္ခပေးလိုရင် ပါဝင်တဲ့ Node ထက်ဝက်ကျော်ထက် ပိုတဲ့ စွမ်းဆောင်ရည် ရှိမှရပါတယ်။ Proof of Stake မှာတော့ ရှိရှိသမျှ ကွိုင်တွေရဲ့ 51% ကို ကိုင်ထားသူက 51% Attack လုပ်မယ်ဆိုရင် ရနိုင်ပါတယ်။ ဒါလည်းပဲ ဖြစ်နိုင်ခြေနည်းပေမယ့် ဒီသဘောရှိတယ်ဆိုတာကိုတော့ သတိပြုရပါလိမ့်မယ်။

Ethereum ကတော့ Version 2.0 အနေနဲ့ အဆင့်မြှင့်တင်တဲ့အခါ တစ်ခြားဖြည့်စွက်နည်းပညာတွေနဲ့အတူ Mining လုပ်ငန်းစဉ်အတွက် Proof of Stake နည်းစနစ်ကို အသုံးပြုတော့မှာပါ။ အခုကတည်းက အစပြုနေပြီဆိုပေမယ့် ဘယ်နေ့မှာ အတည်ပြုအသုံးပြုနိုင်မလည်းဆိုတာကို ရက်အတိအကျ မကြေညာနိုင်သေးလို့ မျှော်တဲ့သူတွေက မျှော်သလို စိတ်ပူတဲ့သူတွေကလည်း ပူနေကြပါတယ်။ ဒါကိုသာ သေသေချာချာ အကောင်အထည်ဖော် နိုင်မယ်ဆိုရင် Ethereum ဟာ အခုထက်ပို အောင်မြင်သွားမှာပါ။

Cardano (ADA)

Cardano ကို Ethereum ရဲ့ ပူးတွဲတည်ထောင်သူတစ်ဦးဖြစ်တဲ့ Charles Hoskinson က ဖန်တီးထားပါတယ်။ Charles Hoskinson ဟာ Vitalik Buterin နဲ့ လုပ်ငန်းဖွဲ့စည်းပုံကိစ္စ ကတောက်ကဆဖြစ်ပြီး Ethereum ကနေ ထွက်ခွာသွားခဲ့တာပါ။ Charles Hoskinson က Ethereum အတွက် Venture Capital တွေရဲ့ ရင်းနှီးမြှုပ်နှံမှုတွေကို လက်ခံပြီး ပုံမှန်လုပ်ငန်းတစ်ခုအနေနဲ့ ဆက်သွားစေချင်ပေမယ့် Vitalik က Non-profit လုပ်ငန်း ပုံစံသာ ဆက်သွားချင်တဲ့အတွက် အဆင်မပြေခဲ့ကြတာပါ။

Cardano ဟာ Proof of Stake ကို လက်ရှိအသုံးပြုထားတဲ့ နည်းပညာ ဖြစ်ပြီး စနစ်တကျ Peer Review လုပ်ထားတဲ့ သုတေသနစာတမ်းတွေပေါ်မှာ အခြေခံတီထွင်ထားတယ်လို့ ဆိုပါတယ်။ Cardano ဆိုတဲ့ အမည်ဟာ သင်္ချာ၊ ရူပဗေဒ၊ ဓာတုဗေဒ၊ အာကာသသိပ္ပံ၊ အတွေးအခေါ် စသည်ဖြင့် ဘာသာရပ်စုံ စွယ်စုံရ အီတလီပညာရှင်တစ်ဦးဖြစ်တဲ့ Gerolamo Cardano ကို အစွဲပြုပြီး ပေးထားတာပါ။ Ethereum နဲ့ Ether ကွဲပြားသလိုပဲ Cardano ဟာ နည်းပညာဖြစ်ပြီး အဲ့ဒီနည်းပညာကို သုံးထားတဲ့ Cryptocurrency ကို ADA လို့ ခေါ်ပါတယ်။ ဒီအမည်ကလည်း Ada Lovelace လို့ခေါ်တဲ့ ပထမဆုံး ကွန်ပျူတာပရိုဂရမ်မာ အမျိုးသမီး ကို အစွဲပြုပြီး ပေးထားတာပါ။

Cardano ဟာ Cryptocurrency တွေမှာရှိနေတဲ့ Scalability ပြဿနာနဲ့ အစိုးရအသိအမှတ်ပြုမှု ပြဿနာ တွေကို ဖြေရှင်းဖို့ ရည်ရွယ်ထားတဲ့ ပရောဂျက်တစ်ခုပါ။ အစိုးရပိုင်းက Cryptocurrency ဆိုတာကို စိုးရွံ့ စရာတစ်ခုလို သဘောထားနေချိန်မှာ သူက အစဉ်အလာစနစ်တွေနဲ့ အရမ်းကင်းကွာသွားတာမျိုး မဖြစ်စေ ပဲ အစိုးရပိုင်းက လက်ခံနိုင်တဲ့စနစ်မျိုး ဖြစ်ဖို့ကို အားထုတ်ဖို့ ရည်ရွယ်ထားပါတယ်။ လက်ရှိ ဈေးကွက်တန် ကြေး Market Cap (၄၅) ဘီလီယံနဲ့ အကြီးဆုံး Cryptocurrency ပရောဂျက်တစ်ခုထဲမှာ အပါအဝင်ဖြစ်ပါ တယ်။

Ethereum လိုပဲ ရည်မှန်းချက်ကြီးမားတဲ့ ပရောဂျက်တစ်ခုဖြစ်ပြီး Cardano ကို စိတ်ဝင်စားကြသူတွေက Ethereum က Second Generation Cryptocurrency ဖြစ်ပြီးတော့ Cardano က Third Generation Cryptocurrency ဖြစ်တယ်လို့ ဆိုကြပါတယ်။

Polkadot (DOT)

Polkadot ဟာလည်း နောက်ထပ် Ethereum ရဲ့ ပူးတွဲတည်ထောင်သူ တစ်ဦးဖြစ်တဲ့ ကွန်ပျူတာသိပ္ပံပညာရှင် Dr. Gavin Wood တည်ထောင်ထားတဲ့ နည်းပညာပါ။ သူဟာ Ethereum ရဲ့ CTO ဖြစ်ခဲ့ပြီး Smart Contract ကုဒ်တွေ ရေးရတဲ့ Solidity ခေါ် Programming Language ကို ဝိုင်းဝန်း ဒီဇိုင်းလုပ်ပေးခဲ့သူပါ။

Ethereum ကနေ ထွက်ခွာလာပြီးတဲ့နောက်မှာ Web3 ဆိုတဲ့ Concept အသုံးအနှုန်းနဲ့အတူ Polkadot ကို အနာဂါတ်အင်တာနက်နည်းပညာတစ်ခု အနေနဲ့ တီထွင်ခဲ့တာပါ။ သူလည်းပဲ Proof of Stake နည်းပညာ

တစ်ခုပါ။ Polkadot ပလက်ဖောင်းကို အသုံးပြုပြီး Blockchain App တွေ ဖန်တီးနိုင်သလို အွဲဒီလိုဖန်တီးထားတဲ့ Blockchain အချင်းချင်း အပြန်အလှန် ဆက်သွယ် အလုပ်လုပ်နိုင်စေတဲ့ Parachain နည်းပညာကိုလည်း တီထွင်ထားပါတယ်။ အတော်လေးဆန်းကျယ် အဆင့်မြင့်တဲ့ Decentralized Application Development Platform ဖြစ်သွားပါပြီ။ အထူးသဖြင့် Blockchain Developer တွေ ပိုစိတ်ဝင်စားကြပါလိမ့်မယ်။

Ethereum တို့ Cardano တို့ Polkadot တို့ရဲ့ ဆန်းသစ်တီထွင်မှုတွေနဲ့အတူ Cryptocurrency ဆိုတာ ငွေကြေးကဏ္ဍတစ်ခုထဲအတွက် မဟုတ်တော့ပါဘူး။ Decentralized အင်တာနက်လို့ ဆိုရမယ့် အများကြီးကျယ်ပြန့်တဲ့ အရာတစ်ခု ဖြစ်နေပါပြီ။ Polkadot ဟာလည်း လက်ရှိ Market Cap ဒေါ်လာ (၁၆) ဘီလီယံနဲ့ အကြီးဆုံး Cryptocurrency ပရောဂျက်တွေထဲမှာ တစ်ခုအပါအဝင်ပဲ ဖြစ်ပါတယ်။

Binance Coin (BNB)

BNB ဟာ Binance က သူ့ Exchange မှာ အသုံးပြုဖို့ ဖန်တီးလိုက်တဲ့ Cryptocurrency တစ်ခုဖြစ်ပါတယ်။ Ethereum Blockchain ပေါ်မှာ ERC-20 Token အနေနဲ့ Token သန်း (၁၀၀) ကို ဖန်တီးပြီး အစပြုခဲ့တာပါ။ အခုတော့ Ethereum ပုံစံတူ လုပ်ထားတဲ့ Binance Chain လို့ခေါ်တဲ့ နည်းပညာကို အသုံးပြုထားတာ ဖြစ်သွားပါပြီ။

ERC-20 Token တွေအတွက် ETH နဲ့ Gas Fee ပေးရသလို Binance Chain Token တွေအတွက် Transaction Fee ကို BNB နဲ့ ပေးရပါတယ်။ ထူးခြားချက်အနေနဲ့ Binance Exchange မှာ Cryptocurrency တွေ အရောင်းအဝယ်လုပ်တဲ့အခါ ကော်မရှင်ကို BNB နဲ့ပေးရင် Discount ပေးတာတို့၊ Binance Chain Token တွေနဲ့ ပစ္စည်းတွေ ဝန်ဆောင်မှုတွေ ဝယ်ရင် Discount ပေးတာတို့လို အခွင့်အရေးတွေကို ပေးပါတယ်။ နောက်ထပ် ထူးခြားချက်အနေနဲ့ (၄) လတစ်ကြိမ် Binance ရဲ့အမြတ် ငါးပုံတစ်ပုံကို BNB တွေပြန်ဝယ်ပြီး Burn ပေးပါတယ်။ ဒါကြောင့် Binance Exchange အမြတ်များများရနေရင် BNB လည်း ဈေးလိုက်တက်နေလိမ့်မယ်ဆိုတဲ့ သဘောပဲဖြစ်ပါတယ်။

လက်ရှိ Market Cap အရ BNB ဟာ စတုတ္ထနေရာမှာ ဒေါ်လာ (၄၈) ဘီလီယံကျော်နဲ့ လိုက်နေလို့ အကြီးဆုံး Cryptocurrency တွေထဲမှာ တစ်ခုအပါအဝင်ပဲဖြစ်ပါတယ်။

Ripple (XRP)

Ripple ဟာ ဟိုးအရင်ကတည်းကရှိနေတဲ့ ငွေကြေးဝန်ဆောင်မှုလုပ်ငန်းတစ်ခုဖြစ်ပြီး သူ့လုပ်ငန်းမှာ အသုံးပြုဖို့အတွက် XRP လို့ခေါ်တဲ့ Cryptocurrency Token ကို တီထွင်ခဲ့တာပါ။ နိုင်ငံရပ်ခြင်း ငွေလွှဲပို့မှု၊ ငွေပေးခြေမှုတွေမှာ ကြားခံထားဖို့ ရည်ရွယ်ချက်နဲ့ ဖြစ်ပါတယ်။ ဥပမာ – စင်ကာပူဒေါ်လာ နဲ့ ထိုင်းဘတ် ကို တိုက်ရိုက်လဲလို့မရ ဖြစ်နေလို့ ဒေါ်လာအရင်လဲပြီးမှ ပြန်လဲရရင် လဲခတွေ နှာပါတယ်။ အဲ့ဒီလိုဖြစ်မယ့်အစား စင်ကာပူဒေါ်လာနဲ့ XRP ကို အရင်ဝယ်ယူပြီးမှ XRP နဲ့ ထိုင်းဘတ်ကို ပြန်လဲတာမျိုးတွေ လုပ်လို့ရဖို့အတွက် ဖြစ်ပါတယ်။ ဒါကြောင့် XRP ဟာ အများဝင်ပြီး Mine လုပ်ယူရတဲ့ Cryptocurrency အမျိုးအစား မဟုတ်ပါဘူး။ Ripple က ကြိုတင်ဖန်တီးပြီးမှ သူ့လုပ်ငန်းရဲ့ အာမခံချက်နဲ့ ထုတ်ရောင်းတဲ့ Token အမျိုးအစားဖြစ်ပါတယ်။

Transaction တွေကို သိမ်းဆည်းဖို့အတွက် Blockchain နည်းပညာကိုသုံးထားပေမယ့် တစ်ခြား Proof of Work Blockchain တွေ Proof of Stake Blockchain တွေနဲ့ အလုပ်လုပ်ပုံ မတူပါဘူး။ Ripple Consensus Algorithm လို့ခေါ်တဲ့ သူ့ကိုယ်ပိုင် နည်းစနစ် တစ်မျိုးကို သုံးပါတယ်။ Distributed Ledger အနေနဲ့ Ledger ကို Node အများအပြားမှာ မိတ္တူကူးပြီး သိမ်းပေမယ့် သူခွင့်ပြုတဲ့ Node တွေပဲ ပါဝင်ခွင့်ရှိပါတယ်။ Transaction တွေ အတွက် Block အသစ် ထည့်ပေးရင်လည်း တစ်ခြား Blockchain တွေမှာလို ဆုငွေ မရပါဘူး။

လက်ရှိမှာ Ripple ဟာ အမေရိကန် Securities and Exchanges Commission (SEC) ရဲ့ တရားစွဲဆိုမှုကို ခံထားရပါတယ်။ SEC ထံမှာ Security အနေနဲ့ မှတ်ပုံတင်ထားခြင်းမရှိဘဲ XRP Token တွေ ထုတ်ရောင်းတဲ့အတွက်ကြောင့်ပါ။ <u>Currency ကို အရောင်းအဝယ်လုပ်ခွင့်ရှိပေမယ့် စတော့လို Security မျိုးကို SEC ရဲ့ ခွင့်ပြုချက်မရှိဘဲ ထုတ်ရောင်းခွင့်မရှိပါဘူး</u>။ Ripple က XRP ဟာ Currency လို့ ဆိုပါတယ်။ SEC ကတော့ Currency မဟုတ်ဘူး၊ Security သာဖြစ်တယ်ဆိုပြီး တရားစွဲထားတာပါ။ ရလဒ်ဘယ်လိုလာဦးမလဲ မသိရသေးပါဘူး။

ဒါဖြင့်ရင် ဘာကြောင့် BTC တို့ ETH တို့ကျတော့ တရားစွဲမခံရတာလည်းလို့ မေးစရာရှိနိုင်ပါတယ်။ BTC တို့ ETH တို့ဟာ ဗဟိုထိမ်းချုပ်မှု မရှိတဲ့အတွက် သူ့ရဲ့ဈေးနှုန်းအတက်အကျကို အဖွဲ့အစည်းတစ်ခုက ထိန်းချုပ်ထားတာ မဟုတ်လို့ SEC ရဲ့ Security ဥပဒေနဲ့ လွတ်ပါတယ်။ XRP ကတော့ ဈေးအတက်အကျဟာ Ripple ပေါ်မှာ မူတည်သလို ဖြစ်နေလို့ ညိနေတာပါ။

XRP ဟာလည်း လက်ရှိ Market Cap ဒေါ်လာ (၃၃) ဘီလီယံကျော်နဲ့ အကြီးဆုံး Cryptocurrency တစ်ခု ဖြစ်နေပါတယ်။ Vitalik Buterin ဟာ Ethereum ကို မတည်ထောင်ခင် Ripple မှာ အလုပ်လျှောက်ခဲ့ဖူးပါတယ်။ အလုပ်ရပါတယ်။ ဒါပေမယ့် အဲ့ဒီအချိန်တုံးက ဗီဇာမရခဲ့လို့ မလုပ်ဖြစ်ခဲ့လိုက်တာပါ။

Uniswap (UNI)

Cryptocurrency တွေကို ရောင်းဝယ်လဲလှယ်လိုတဲ့အခါ Exchange တွေကို အသုံးပြုကြရပါတယ်။ ဗဟိုထိန်းချုပ်စနစ်ကို မကြိုက်လို့ ထွင်ခဲ့ကြပေမယ့် Exchange တွေက ဗဟိုကဲ့သို့ ပြန်ဖြစ်လာပါတယ်။ ဒီလိုမျိုး မဖြစ်ရအောင် Decentralized Exchange နည်းပညာတွေ ရှိနေပါတယ်။ ဗဟို Exchange မလိုပဲ Cryptocurrency တစ်ခုနဲ့တစ်ခု အပြန်အလှန် လဲလို့ရစေတဲ့ နည်းပညာပါ။ Uniswap ဟာ လက်ရှိ Decentralized Exchange နည်းပညာထဲမှာ နံပါတ် (၁) ဖြစ်နေပါတယ်။

Uniswap ကို Ethereum Blockchain ပေါ်မှာပဲ Smart Contract အနေနဲ့ ဖန်တီးထားတာ ဖြစ်ပါတယ်။ ဒါကြောင့် ERC-20 Token အားလုံး Uniswap နဲ့ အပြန်အလှန် အလဲအလှယ် လုပ်နိုင်ပါတယ်။ ဥပမာ – လက်ရှိပေါက်ဈေးက 1 ETH = 10 BAKE ဆိုကြပါစို့။ ပုံမှန်ဆိုရင် ကိုယ့်မှာ 10 BAKE ရှိနေရင် အဲ့ဒီ 10 BAKE ကို 1 ETH နဲ့လဲချင်တဲ့အခါ လဲပေးမယ့်သူကို ရှာရမှာပါ။ Uniswap ကတော့ အဲ့ဒီလို လိုက်ရှာနေစရာမလိုအောင် Exchange Pair Pool တွေ ဖန်တီးပြီး အလုပ်လုပ်ပါတယ်။ ဥပမာ – ETH/BAKE လို့ခေါ်တဲ့ Pool တစ်ခုရှိပြီး အလဲအလှယ် လုပ်လိုသူတွေက အဲ့ဒီ Pool ထဲကို ကိုယ့်ရဲ့ BAKE ကိုထည့်ပြီး တန်ဖိုးညီမျှတဲ့ ETH ကို ပြန်ထုတ်ယူလို့ ရသွားတဲ့သဘောပါ။ ဒါကြောင့် အတိအကျ လဲပေးချင်တဲ့သူကို စောင့်နေစရာမလိုတော့ဘဲ Uniswap Pool ထဲမှာ ဝင်ပြီး အလဲအလှယ် လုပ်လို့ရသွားတဲ့သဘောပါ။

ဈေးအတက်အကျအနေနဲ့ Pool ထဲမှာ ETH နည်းသွားရင် ETH ဈေးအလိုလို တက်သွားမှာဖြစ်ပြီး၊ BAKE နည်းသွားရင် BAKE ဈေးအလိုလို တက်သွားမှာဖြစ်ပါတယ်။ အပြန်အလှန်အားဖြင့် BAKE ဝင်ထည့်တဲ့သူများလာရင် BAKE ဈေးက ကျလာမှာပါ။ အဲ့ဒါကို အလိုအလျှောက် တွက်ပေးတဲ့ ဖော်မြူလာရှိပါတယ်။ အတော်စိတ်ဝင်စားဖို့ ကောင်းတဲ့ နည်းပညာတစ်ခုပါပဲ။

BAKE ဆိုတာ စိတ်ကူးယဉ် Cryptocurrency ပါ။ တစ်ကယ်မရှိပါဘူး။ ERC-20 အကြောင်းပြောတော့ နမူနာတစ်ခုအနေနဲ့ ထည့်ပြောခဲ့လို့ ပြန်သုံးလိုက်တာပါ။ သတိမထားမိရင် ပြန်လိုက်ရှာနေမှာစိုးလို့ပါ။

Uniswap ရဲ့ UNI ဆိုတာကတော့ ERC-20 Token ပဲဖြစ်ပြီး UNI Token လက်ဝယ်ရှိသူတွေဟာ Uniswap ရဲ့ အလုပ်လုပ်ပုံနဲ့ ပက်သက်ပြီး ပြင်ဆင်လိုတာ၊ အဆင့်မြှင့်တင်လိုတာတွေရှိရင် Vote လုပ်ခွင့်ရမယ့်သူတွေ ဖြစ်ပါတယ်။ Uniswap ကို အသုံးပြုသူတွေကို UNI Token တွေ ဝေပေးထားပါတယ်။

Solana (SOL)

Solana ဟာ Block အသစ်ထည့်ဖို့ အချိန် (၄၀၀) မီလီစက္ကန့်သာ လိုအပ်ပြီး၊ တစ်စက္ကန့်ကို Transaction (၅၀,၀၀၀) ထိ အလုပ်လုပ်ပေးနိုင်တဲ့ Cryptocurrency နည်းပညာလို့ ဆိုပါတယ်။ အများကြီး မြန်သွားပါပြီ။ Proof of Stake ကိုအခြေခံထားတဲ့ Proof of History လို့ခေါ်တဲ့ စနစ်ကို အသုံးပြုပါတယ်။

ပုံမှန်အားဖြင့် တစ်ခြား Blockchain တွေမှာ Transaction တွေကို Block ထဲမှာ စုထည့်ပြီး သိမ်းကြပါတယ်။ Blockchain နည်းပညာအရ Block တွေ Valid ဖြစ်မဖြစ် စစ်ရတာ မြန်ပါတယ်။ တစ်ခုနဲ့တစ်ခု Hash နဲ့ ချိတ်ဆက်ထားလို့ Hash ကိုစစ်ကြည့်လိုက်ယုံပါပဲ။ ဒီအကြောင်းကို ရှေ့ပိုင်းမှာ ရှင်းပြခဲ့ပြီးသားပါ။ ဒါပေမယ့် Block ထဲက စုထည့်ထားတဲ့ Transaction တွေ Valid ဖြစ်မဖြစ် စစ်ရတာတော့ အချိန်ယူရပါတယ်။ Node တစ်ခုက Blockchain Update ရှိကြောင်း Broadcast ကို လက်ခံရရှိတိုင်း Transaction တွေ မှန်မမှန် နောက်ကြောင်းပြန်ပြီး လိုက်စစ်နေရတာပါ။

Solana က အဲ့ဒီပြဿနာကိုဖြေရှင်းဖို့ Transaction တွေကို သိမ်းတဲ့အခါ ပြီးခဲ့တဲ့ Transaction ရဲ့ Hash နဲ့ တွဲပြီးသိမ်းပါတယ်။ Blockchain ဖြစ်ယုံသာမက Transaction Chain ဖြစ်သွားတာပါ။ Block တစ်ခု Valid ဖြစ်မဖြစ် Hash ကို ကြည့်နိုင်သလိုပဲ Transaction တစ်ခု Valid ဖြစ်မဖြစ်ကိုလည်း Hash ကိုကြည့်လိုက်ယုံနဲ့ ရနိုင်လို့ ပိုမြန်သွားပါတယ်။ ဒီသဘောကို Proof of History လို့ခေါ်တာပါ။ ဒီသဘောကြောင့်ပဲ ရိုးရိုး Proof of Stake ထက်တောင် သူကပိုမြန်သွားသေးတဲ့ သဘောဖြစ်နေတာပါ။

Solana ဟာလည်း လက်ရှိ Market Cap ဒေါ်လာ (၉) ဘီလီယံကျော် ရှိနေတဲ့ အဓိက Cryptocurrency နည်းပညာတစ်ခုပဲ ဖြစ်ပါတယ်။

Chainlink (LINK)

Ethereum ရဲ့ Smart Contract တီထွင်မှုနဲ့အတူ Blockchain ဆိုတာ အချက်အလက် သိမ်းဆည်းယုံသက်သက် မဟုတ်တော့ဘဲ အခြေအနေပေါ်မူတည်ပြီး လိုအပ်သလို အလို အလျှောက် လုပ်ဆောင်ချက်တွေ ပါဝင်နိုင်တဲ့ Decentralized Application Platform ဖြစ်လာခဲ့ပါပြီ။ ဒါဟာ Blockchain ကို အသုံးပြုပြီး အသုံးချဆော့ဖ်ဝဲတွေ ဖန်တီးလိုက်တာပါပဲ။ ဆော့ဖ်ဝဲ တစ်ခု အလုပ်လုပ်ဖို့အတွက် Data လိုပါတယ်။ Data တိုင်းက Blockchain ထဲမှာ ရှိနေတာ မဟုတ်ပါဘူး။ Blockchain ရဲ့ပြင်ပမှာ ရှိနေတဲ့ Off-Chain Data တွေကိုလည်း Smart Contract နဲ့အတူ တွဲဖက် အသုံးပြုဖို့ လိုအပ်နိုင်ပါတယ်။

Blockchain ရဲ့ ပြင်ပမှာရှိနေတဲ့ Off-Chain Data တွေကို ရယူပေးနိုင်တဲ့ Smart Contract တွေကို Data Oracle လို့ ခေါ်ပါတယ်။ ဒီ Data Oracle တွေရဲ့ ပြဿနာက Data လိုအပ်တဲ့ Smart Contract တွေက သူ ကို မှီခိုနေရလို့ သူက ဗဟိုချက်တစ်ခု ပြန်ဖြစ်နေတာပါပဲ။ သူကိုယ်တိုင်ကလည်း ဗဟို Data Source နေ Data ကို ရယူနေရပါသေးတယ်။ ဗဟိုထိန်းချုပ်မှုကို မလိုလားတဲ့ Decentralize စနစ်တွေရဲ့ မူနဲ့ မကိုက်ညီ သလို ဗဟိုချက်မှာ ပြဿနာတက်တာနဲ့ မှီခိုနေရသူ အားလုံး ဒုက္ခရောက်ကြပါတော့မယ်။

Chainlink ကတော့ Oracle Node တွေ ဝိုင်းဝန်းချိတ်ဆက် ပါဝင်နိုင်တဲ့ Oracle Network တစ်ခု ဖြစ်ပြီး သတ်မှတ် စည်းကမ်းချက်များနဲ့အညီ တိကျမှန်ကန်တဲ့ Data ကို ယူပေးရင် ဆုအနေနဲ့ LINK Token တွေပေးတဲ့နည်းနဲ့ အချက်အလက်ရဲ့ ယုံကြည်စိတ်ချရမှုကို အာမခံချက်ပေးမယ့် နည်းပညာဖြစ်ပါတယ်။ သူလည်းပဲ Decentralized App တွေအတွက် အရေးပါတဲ့ နည်းပညာတစ်ခုပါပဲ။

Chainlink ကို ERC-677 လို့ခေါ်တဲ့ Ethereum Token နည်းပညာအသုံးပြု ဖန်တီးထားပေမယ့် ဘယ် Blockchain နဲ့မဆို တွဲဖက်အသုံးပြုလို့ရနိုင်ပါတယ်။

Polygon (MATIC)

Polygon ဟာ ကိုယ်တိုင် Blockchain နည်းပညာဖန်တီးဖို့အတွက် လိုအပ်တာတွေအသင့် စုစည်းပေးထားတဲ့ Framework တစ်ခု ပါ။ Polygon ဟာလည်း စွမ်းဆောင်ရည်မြင့် Decentralized App တွေဖန်တီးဖို့အတွက် ရည်ရွယ်ထားတာမို့လို့ နည်းပညာအားဖြင့် လေးနက်ရှုပ်ထွေးပေမယ့် သူ့သဘောအနှစ်ချုပ်က ဒီလိုပါ။

Ethereum ဟာ လက်ရှိအချိန်ထိ Proof of Work ကိုသာ အသုံးပြုနေရသေးလို့ နှေးပါတယ်။ ဒါကြောင့် Polygon ကို အသုံးပြုပြီး ပိုမြန်တဲ့ Proof of Stake Blockchain တစ်ခုကို Ethereum ပေါ်မှာပဲ နောက် Layer တစ်ခုအနေနဲ့ ထပ်ဆင့် တည်ဆောက်နိုင်ပါတယ်။ ဒါကြောင့် လုပ်စရာရှိတဲ့ Transaction တွေကို ပို မြန်တဲ့ ထပ်ဆင့် Blockchain ပေါ်မှာ လုပ်သွားပြီး၊ အဲ့ဒီအချက်အလက်တွေကို စုစည်းပြီး နောက်ကွယ်မှာ ပင်မ Ethereum Blockchain ထဲကို ထည့်သိမ်းသွားလို့ ရနိုင်ပါတယ်။ ဒါကြောင့် ထပ်ဆင့် Layer ကပေးတဲ့ Transaction Speed အားသာချက်ကိုရပြီး နောက်ကွယ် Layer ဖြစ်တဲ့ Ethereum ကပေးတဲ့ ခိုင်မာမှုကို လည်း ရရှိသွားပါတယ်။ နေရာတကာ ပင်မ Blockchain ကို စောင့်နေစရာမလိုတော့ဘဲ ကြိုလုပ်လို့ရတဲ့၊ သီးခြားလုပ်လို့ရတဲ့ အလုပ်တွေကို Sidechain ခေါ် ထပ်ဆင့် Layer အနေနဲ့ တည်ရှိတဲ့ Blockchain ပေါ် မှာ မြန်မြန်ဆန်ဆန် လုပ်လို့ရသွားတာပါ။

ဒီလိုသဘောမျိုးရှိလို့ <u>Polygon ကို Layer-2 Scaling Solution လို့ ခေါ်ပါတယ်</u>။ Polygon ကိုအသုံးပြုပြီး ကိုယ့်လိုအပ်ချက်နဲ့ ကိုက်ညီတဲ့ Blockchain တွေကို အလွယ်တစ်ကူ Customize လုပ်ပြီး တည်ဆောက် အသုံးပြုနိုင်မှာဖြစ်ပါတယ်။ Polygon ရဲ့ MATIC Token ကိုတော့ ဒီလိုတည်ဆောက်အသုံးပြုတဲ့ Blockchain တွေမှာ ပြုလုပ်တဲ့ Transaction တွေအတွက် Gas Fee အနေနဲ့ အသုံးပြုရပါတယ်။

Monero (XMR)

Bitcoin လို Cryptocurrency မျိုးဟာ ကိုယ်ဘယ်သူဘယ်ဝါ ပြောစရာမလိုဘဲ၊ တိုက်ရိုက် ဖလှယ်အသုံးပြုနိုင်လို့ Privacy ကောင်းတယ်လို့ ဆိုနိုင်ပါတယ်။ ဒါပေမယ့် အခြားတစ်ဘက် မှာလည်း ကိုယ်ပြုလုပ်လိုက်တဲ့ Transaction တိုင်းဟာ Network ထဲမှာ မည်သူမဆို ကြည့် လို့ရနေတဲ့ ပြဿနာ ကလည်း ရှိနေပြန်ပါတယ်။ Network ထဲမှာ လူပုဂ္ဂိုလ်ဆိုင်ရာ အချက်အလက်တွေ မ ပါပေမယ့် Address တစ်ခုရဲ့ ငွေပေးချေမှု မှတ်တမ်းကို အစအဆုံး အကုန်လိုက်လို့ရနေပါတယ်။

Monero ကတော့ Transaction ပြုလုပ်လိုက်တဲ့အခါ ပေးပို့သူရဲ့ Address ကို တိုက်ရိုက် အသုံးမပြုဘဲ Stealth Address လို့ခေါ်တဲ့ Address တစ်ခု ဖန်တီးအသုံးပြုခြင်း အားဖြင့် မူရင်း Address ရဲ့ နောက်ကြောင်းကို လိုက်လို့မရအောင် အလုပ်လုပ်ပေးပါတယ်။ ဒါကြောင့် Monero လို Cryptocurrency မျိုးကို Privacy Coin လို့ ခေါ်ကြပါတယ်။

ဒီအချက်ကြောင့် Privacy ပိုကောင်းသွားခြင်းနဲ့အတူ ဒုစရိုက်လောကသားတွေရဲ့ မျက်စိကျခြင်းကိုလည်း ခံနေရပါတယ်။ Darkweb Market မှာ Bitcoin ထက်စာရင် Monero ကို ပိုပြီးတော့ သုံးလာကြသလို အမေရိကန် အခွန်ဌာန IRS က Monero ကုဒ်ကို ဖော်နိုင်ရင် ဒေါ်လာ (၆) သိန်းကျော် ဆုချမယ်လို့တောင် ကြေညာထားရပါတယ်။

အာဏာပိုင်တွေရဲ့ ဖိအားပေးမှုကြောင့် တချို့ Exchange တွေကလည်း Monero ကို အရောင်းအဝယ်လုပ်ခွင့်မပြုကြသလို အရင်ခွင့်ပြုထားတဲ့ Exchange တွေကလည်း ခွင့်မပြုတော့ဘဲ ပြန်ဖြုတ်ချကြတာတွေ ရှိပါတယ်။

Stable Coins (USDT, USDC, BUSD)

Stable Coin ဆိုတာဟာ ပြင်ပက Fiat Money နဲ့ တိုက်ရိုက်ချိတ်ဆက်ထားတဲ့ Token တွေပါပဲ။ (၁၀) ဒေါ်လာပေးရင် အဲ့ဒီ ဒေါ်လာကို သိမ်းထားပြီး Token (၁၀) ခု ထုတ်ပေးလိုက်တဲ့ သဘောပါပဲ။ နောင် Token တွေ ပြန်အပ်လိုက်ရင် သိမ်းထားတဲ့ ဒေါ်လာကို ပြန်ထုတ်ပေးလိုက်မှာပါ။

သူ့မှာ ဈေးနှုန်းအတက်အကျရယ်လို့ မရှိပါဘူး။ ဒါကြောင့် Stable Coin လို့ ခေါ်တာပါ။ ဒီလိုဈေးနှုန်းအတက်အကျမရှိစေဖို့အတွက် Stable Coin ထုတ်ပေးတဲ့အဖွဲ့အစည်းက ကွိုင် (၁) သန်းထုတ်ပေးထားရင် ဘဏ်အကောင့်ထဲမှာ ဒေါ်လာ (၁) သန်းကို အတိအကျ ထည့်သိမ်းထားပေးရပါတယ်။ ဒါကြောင့် သူ ထုတ်ပေးထားတဲ့ ကွိုင် (၁) သန်းဟာ အမှန်တစ်ကယ် တစ်ကွိုင်ကို (၁) ဒေါ်လာတန်တယ်ဆိုတဲ့ အာမခံချက်ကို အမြဲရနေမှာပါ။ ဒီလိုမျိုး အမှန်တစ်ကယ် အရန်ငွေကို အတိအကျ သိမ်းထားပေးပါတယ် ဆိုတာကို ပြင်ပစာရင်းစစ်တွေနဲ့ အမြဲအစစ်ခံပေးရပါတယ်။ ဒါကြောင့် Stable Coin တွေဟာ အမှန်တစ်ကယ် ပြင်ပငွေနဲ့ တူညီတဲ့တန်ဖိုးမှာ အမြဲရှိနေမှာပါ။

Stable Coin တွေကို ဒေါ်လာအစားထိုး Cryptocurrency အနေနဲ့ Wallet ထဲမှာ ထည့်သိမ်းတာ၊ ပေးပို့တာ၊ လဲလှယ်တာတွေ လုပ်လို့ရနိုင်ပါတယ်။ အဲ့ဒီလို Stable Coin တွေထဲမှာ လက်ရှိ Market Cap အရ အဓိကကျနေတာတွေကတော့ Tether (**USDT**), USD Coin (**USDC**) နဲ့ Binance USD (**BUSD**) တို့ပဲဖြစ်ပါတယ်။

Tether (**USDT**) ကို Biftinex လို့ခေါ်တဲ့ ဟောင်ကောင်အခြေစိုက် Exchange က ထုတ်ပေးထားတာပါ။ Market Cap ဒေါ်လာ (၆၂) ဘီလီယံကျော်ရှိလို့ BTC နဲ့ ETH ပြီးရင် တတိယမြောက် အကြီးဆုံး Cryptocurrency ဖြစ်နေပါတယ်။ Teather ဟာ လက်ရှိမှာ ဝေဖန်မှုပေါင်းများစွာကို ခံနေရပြီး သူ့ရဲ့ စိတ်ချယုံကြည်ရမှုကိုလည်း မေးခွန်းထုတ်နေကြပါတယ်။

(၂၀၁၇) ခုနှစ်က ဟက်ခံခဲ့ရသလို၊ (၂၀၁၈) ခုနှစ်မှာ ပြင်ပစာရင်းစစ်ကို အစစ်မခံလို့ အာဏာပိုင်တွေက တရားရုံးအမိန့်နဲ့ ဆင့်ခေါ်ပြီး စာရင်းတွေ စစ်ခဲ့ရပါတယ်။ (၂၀၁၉) ခုနှစ်မှာလည်း Tether ရဲ့ ပင်မကုမ္ပဏီက Tether ရဲ့ အရန်ငွေတွေကို တစ်ဖက်လှည့်နဲ့ ယူသုံးထားတယ်လို့ နယူးယောက်ရှေ့နေချုပ်က စွဲဆိုတာခံရလို့ ရင်ဆိုင်ဖြေရှင်းရပါသေးတယ်။ အခုနောက်ဆုံးအနေနဲ့ ကွိုင်နဲ့ ငွေသားကို ချိတ်ထားဖို့အတွက် (၁၀၀%) Cash Reserve မရှိဘဲ (၇၅%) သာရှိတယ်လို့ ထုတ်ပြန်ခဲ့လို့ ထပ်ပြီးတော့ ဝေဖန်ခံရပြန်ပါတယ်။ ကျန် (၂၅%) က ရရန်ရှိစာရင်းတွေနဲ့ ဘွန်းစာချုပ်တို့၊ ရွှေတို့၊ Bitcoin တို့ အနေနဲ့ ရှိနေတာပါ။

နောက် Stable Coin တစ်ခုဖြစ်တဲ့ USD Coin (**USDC**) ကတော့ Center လို့ခေါ်တဲ့ အဖွဲ့အစည်းက စီမံနေတဲ့ Stable Coin ဖြစ်ပါတယ်။ အဲ့ဒီအဖွဲ့အစည်းကို Circle လို့ခေါ်တဲ့ ငွေကြေးဝန်ဆောင်မှုကုမ္ပဏီနဲ့ Coinbase Exchange တို့ ပူးပေါင်းတည်ထောင်ထားကြပါတယ်။ USDC ကတော့ လစဉ် စာရင်းအစစ် ခံနေတဲ့ Stable Coin ဖြစ်လို့ ပိုပြီးတော့ စိတ်ချယုံကြည်ရတယ်လို့ လက်ခံထားကြပါတယ်။

Binance USD (**BUSD**) ကိုတော့ New York State Department of Financial Services (NYDFS) ရဲ့ တရားဝင်ခွင့်ပြုချက်အရ Binance Exchange နဲ့ Paxos လို့ခေါ်တဲ့ Blockchain နည်းပညာကုမ္ပဏီတို့ ပူးပေါင်း ဖန်တီးထားတာပါ။ သူလည်းပဲ လစဉ် စာရင်းအစစ်ခံနေတဲ့ Stable Coin ဖြစ်လို့ စိတ်ချယုံကြည်ရပါတယ်။

Stable Coin တွေဟာ တစ်ခြား Altcoin တွေလို နည်းပညာအရ ဆန်းပြားတာမျိုး မဟုတ်ပေမယ့် အရေးပါတဲ့ Cryptocurrency တွေပါ။ ငွေသားကို အမြဲတမ်း ထည့်လိုက်၊ ထုတ်လိုက် လုပ်နေစရာ မလိုအပ်တော့ဘဲ ငွေသားနဲ့ တန်းဖိုးညီတဲ့ Stable Coin ကို ကိုင်ထားနိုင်တဲ့ အတွက်ကြောင့် ကိုယ့်အပိုင် Cryptocurrency တွေကို ပိုပြီးတော့ လွယ်လွယ်လပ်လပ် ကိုင်တွယ်စီမံနိုင်သွားစေမှာပါ။

Dai (DAI)

DAI ဟာလည်း Stable Coin တစ်မျိုးပါပဲ။ ဒါပေမယ့် တစ်ခြား Stable Coin တွေနဲ့ သဘောသဘာဝ မတူတဲ့အတွက် သူ့အကြောင်းကို အခုလိုသပ်သပ်ခွဲပြီး ပြောလိုက်တာပါ။ တစ်ခြား Stable Coin တွေဟာ အဖွဲ့အစည်းတစ်ခုရဲ့ အာမခံချက်နဲ့ သိမ်းထားပေးတဲ့ Cash Reserve ကို Token နဲ့ တည့်ချိတ်ထားပေးလို့ Stable ဖြစ်နေကြတာပါ။ ကွိုင်ရဲ့တည်ငြိမ်မှုဟာ အဲ့ဒီအဖွဲ့အစည်းရဲ့ စီမံမှုပေါ်မှာ မူတည်နေပါတယ်။

DAI ကတော့ ဗဟိုအဖွဲ့အစည်းတစ်ခုက ငြိမ်အောင်ထိန်းထားပေးစရာမလိုဘဲ သူ့အလိုလို ဈေးနှုန်း ငြိမ်နေအောင် Smart Contract နဲ့ Algorithm ထုတ်ပြီး ထိန်းထားတာပါ။ နောက်ကွယ်က အလုပ်လုပ်ပုံက ရှုပ်ထွေးဆန်းကျယ်ပေမယ့် ပုံမှန် အသုံးပြုသူက အဲ့ဒါတွေ သိစရာမလိုပါဘူး။ 1 DAI ကို 1 USD ဝန်းကျင်မှာ အမြဲတမ်း အလဲအလှယ်လုပ်လို့ရနေမှာပါ။

ဝန်းကျင်လို့ ပြောတာက $1 အတိအကျတော့ ရမှာ မဟုတ်ပါဘူး $0.9993 တို့ $1.0008 တို့လောက် အတိုးအလျော့ အလှုပ်အရှားလေးတွေ ရှိနေပါလိမ့်မယ်။ DAI ရဲ့ Smart Contract Algorithm က ပေါက်ဈေး $1 အထက် တက်လာရင် ကျအောင် ပြန်ဆွဲချပေးပြီး၊ $1 အောက် ကျလာရင် တက်အောင် ပြန်ဆွဲတင်ပေးနေတာပါ။ တစ်ခြား Cash Reserve နဲ့ ချိတ်ထားတဲ့ Stable Coin တွေမှာလည်း အဲ့ဒီလို ဈေးနှုန်းအလှုပ်အရှား ရှိတတ်ပေမယ့် DAI ကတော့ သူတို့ထက် နည်းနည်းပို လှုပ်ပါလိမ့်မယ်။

ဈေးနှုန်း အတင်အချ လုပ်ပေးနေတယ်ဆိုတာ ဒီလိုပါ။ လွပ်လပ်တဲ့ ဈေးကွက်ထဲမှာ ရှိနေတဲ့ အရာတစ်ခု ဈေးတက်တယ်၊ ကျတယ်ဆိုတာ၊ အကြောင်းရင်းကတော့ Supply & Demand ကြောင့်ပါပဲ။ ပထမအဆင့် အနေနဲ့ DAI Token အသစ် လိုချင်ရင် ETH (သို့) တစ်ခြားခွင့်ပြုထားတဲ့ Cryptocurrency ကို အပေါင်ထားပြီး ချေးယူရပါတယ်။

ဈေးကွက်ထဲမှာ DAI Token ကို ဝယ်ချင်တဲ့သူ များနေလို့၊ ရှိတဲ့ Supply ထက် Demand က ပိုများနေရင်၊ ဈေးတက်လာမှာပါပဲ။ ဒါထုံးစံပါ။ အဲ့ဒီလို ဈေးတက်လာတဲ့အခါ အပေါင်ထားသူက တက်လာတဲ့ ပမာဏ အတွက် အတိုးရပါတယ်။ ရမယ့် အတိုးကို DAI Token အသစ်တွေ ထပ်ထုတ်ပြီး ပေးလိုက်တဲ့အခါ Supply တွေ ထပ်တိုးလာလို့ Supply နဲ့ Demand ပြန်မျှသွားပြီး ဈေးပြန်ကျသွားစေပါတယ်။

ပြောင်းပြန်အနေနဲ့ ဈေးကွက်ထဲမှာ DAI Token ကို ပြန်ရောင်းတဲ့သူများနေလို့ Demand ကျလာတဲ့အခါ ဈေးလည်း ကျလာမှာပါပဲ။ အဲ့ဒီလိုဈေးကျတဲ့အခါ အပေါင်ထားသူက အတိုးမရတော့ပါဘူး၊ အတိုးပြန်ပေးရမှာပါ။ မပေးချင်ရင် သူ့မှာရှိနေတဲ့ DAI Token တွေကို ပြန်အပ်ပြီး သူ့အပေါင်ကို ပြန်ထုတ်ယူထားဖို့ လိုပါတယ်။ Smart Contract က အဲ့ဒီလို ပြန်အပ်လာတဲ့ Token တွေကို Burn လုပ်ပစ်လိုက်တဲ့အခါ Supply ပြန်ကျသွားတဲ့အတွက် ဈေးလည်းပြန်တက်သွားစေမှာပဲ ဖြစ်ပါတယ်။

ဒီနည်းနဲ့ Supply & Demand ကို အလိုအလျှောက် ညှိပေးသွားလို့ ဈေးနှုန်းက လိုချင်တဲ့ပမာဏမှာ အနီးစပ်ဆုံး ငြိမ်နေတာပါ။ ဒီစနစ်မှာ အပေါင်ထည့်ပေးထားသူတွေလည်း အကျိုးမယုတ်ပါဘူး။ တက်သွားတဲ့ အစွန်းထွက်လေးတွေ၊ ကျသွားတဲ့ အစွန်းထွက်လေးတွေကို အမြတ်ရနေနိုင်တဲ့ အတွက်ကြောင့်ပါ။

ဒါက ထုတ်ပေးတဲ့ DAI ရဲ့ ဈေးအတက်အကျ အကြောင်းပဲ ပြောရပါသေးတယ်။ အပေါင်ပေးပြီး ထည့်ထားတဲ့ ETH လို Cryptocurrency ရဲ့ ဈေးအတက်အကျကလည်း ရှိပါသေးတယ်။ ဒါကြောင့်လည်း က Algorithm ရဲ့ အလုပ်လုပ်ပုံက ဒီထက်ပိုပြီး အများကြီး ဆန်းကျယ် ရှုပ်ထွေးပါလိမ့်မယ်။ တော်တော်လေး စိတ်ဝင်စားဖို့ကောင်းတဲ့ သဘောသဘာဝ တစ်ခုပါ။

ဒါဟာ Decentralized Finance (DeFi) ပရောဂျက်တစ်ခုကို လက်တွေ့ တွေ့မြင်ရခြင်းပါပဲ။ ဗဟိုထိန်းချုပ်မှုမရှိဘဲ လိုချင်တဲ့ ငွေကြေးဝန်ဆောင်မှုကို ရနေတာပါ။ DAI ကို MakerDAO လို့ခေါ်တဲ့ အဖွဲ့အစည်းတစ်ခုက တီထွင်ထားပါတယ်။ သူ့မှာလည်း MKR လို့ခေါ်တဲ့ သီးခြား Cryptocurrency တစ်ခု ရှိပါသေးတယ်။ MKR Token လက်ဝယ်ရှိသူတွေဟာ Dai ရဲ့ အလုပ်လုပ်ပုံနဲ့ ပက်သက်ပြီး ပြင်ဆင်လိုတာ၊ အဆင့်မြှင့်တင်လိုတာတွေရှိရင် Vote လုပ်ခွင့်ရမယ့်သူတွေ ဖြစ်ပါတယ်။

Conclusion

တစ်ကယ်တော့ Steller (XLM), VeChain (VET), Aave (AAVE), Algorand (ALGO), Terra (LUNA), PancakeSwap(CAKE) စသည်ဖြင့် တစ်ခြား စိတ်ဝင်စားဖို့ကောင်းတဲ့ Altcoin တွေမှ အများကြီး ကျန်ပါသေးတယ်။ ဒါက Market Cap မြင့်တာတွေပဲ ရှိပါသေးတယ်။ အခုမှ စတင်တီထွင်လို့ Market Cap သိပ်မရှိသေးပေမယ့် နည်းပညာမြင့်ပြီး အိုင်ဒီယာကောင်းတဲ့ Altcoin တွေလည်း ရှိပါသေးတယ်။

တချို့ Altcoin တွေဟာ စိတ်ဝင်စားစရာ ကောင်းလွန်းလို့ သူ့အကြောင်းချည်းပဲ စာအုပ် တစ်အုပ်လောက် ရေးပြမှာသာ ပြည့်စုံမှာဖြစ်ပါတယ်။ အဲ့ဒီလောက် ကျယ်ပြန့်တဲ့ အကြောင်းအရာတွေထဲကမှ အဓိကကျတာတွေကို ရွေးထုတ်ပြီး အကျဉ်းချုပ် Summary လောက်သာ ဖော်ပြနိုင်ခဲ့တာပါ။ ဒါပေမယ့် ဒီလိုအကျဉ်းချုပ်ဖော်ပြချက်ကနေပဲ စာဖတ်သူအတွက် Cryptocurrency လောကမှာ လက်ရှိ ဘာတွေဖြစ်နေသလဲ ဆိုတာကို Overview အနေနဲ့ ခြုံငုံသိမြင်သွားစေဖို့ အထောက်အကူ ဖြစ်စေလိမ့်မယ်လို့ မျှော်လင့်ပါတယ်။

နိဂုံးချုပ်

စာရေးသူဟာ Bitcoin ပေါ်ခါစက နည်းပညာသမားတစ်ယောက်အနေနဲ့ လက်တွေ့ စမ်းသပ် လေ့လာမှုတွေ လုပ်ဖြစ်ခဲ့ပါတယ်။ နည်းပညာပိုင်းအရ အတော်လေး စိတ်ဝင်စားပေမယ့် သူ့ရဲ့ ငွေကြေးဆိုတဲ့ သဘောသဘာဝကိုတော့ သိပ်နားမလည်တာကြောင့် နောက်ပိုင်းမှာ ဆက်မလုပ်ဖြစ်ခဲ့ပါဘူး။

၂၀၂၀-၂၁ ခုနှစ်တွေမှာ တစ်ကမ္ဘာလုံးလိုလို ပြန့်နှံ့ခဲ့တဲ့ Covid-19 ကပ်ရောဂါကြောင့်၊ နိုင်ငံအသီးသီးရဲ့ Stay At Home ကြေညာချက်တွေနဲ့အတူ၊ လူတွေဟာ ရောဂါကူးစက်မှုနှုန်း ကျစေဖို့အတွက် အလုပ်တွေ၊ ကျောင်းတွေ၊ ရပ်နားပြီး အိမ်ထဲမှာပဲ နေကြရပါတယ်။ ဒီလိုနေရတာ ကာလရှည်ကြာလာတဲ့အခါ အိမ်ထဲမှာပဲနေပြီး ဝင်ငွေရနိုင်မယ့် နည်းလမ်းတွေကို စူးစမ်းရှာဖွေကြရင်း စတော့မားကတ်တို့၊ Cryptocurrency မားကတ်တို့ကို ပိုစိတ်ဝင်စားလာကြပါတယ်။

စာရေးသူလည်း အများနည်းတူ ပြန်စိတ်ဝင်စားလာလို့ ကြားထဲမှာ အဆက်ပြတ်နေတဲ့ Blockchain နည်းပညာတွေနဲ့ Cryptocurrency တွေ အကြောင်းကို ပြန်လေ့လာကြည့်တဲ့အခါ လုံးဝကို အံ့အားသင့်ဖွယ် ကောင်းလောက်အောင် ပြောင်းလဲတိုးတက်နေပြီဆိုတာကို တွေ့လိုက်ရတာပါပဲ။ Currency နဲ့ Finance ဘက်ပိုင်းမှာတင် မကဘဲ အနာဂါတ် အင်တာနက်နည်းပညာကြီး တစ်ခု၊ အနာဂါတ် Development Platform ကြီးတစ်ခုဘက်ကို ဦးတည်နေပြီဆိုတာကို သိလိုက်ရပါတယ်။

ရှင်းနီးမြှုတ်နှံမှုပိုင်းကို သိပ်စိတ်မဝင်စားရင်တောင် စာရေးသူလို နည်းပညာသမား၊ Software Developer တစ်ဦးအတွက်၊ အခုနေမှ မီအောင်မလိုက်ရင် နည်းပညာပိုင်းမှာ အတော်ကြီး ခေတ်နောက်ကျပြီး ပြတ်ကျန်ခဲ့တော့မယ်ဆိုတဲ့ သဘောဖြစ်နေပါတယ်။ ဒါကြောင့် ကိုယ်တိုင်လည်း ကြိုးစားလေ့လာဖြစ်ခဲ့သလို၊

တစ်ခြားလေ့လာသူတွေ အတွက်လည်း၊ ကိုယ့်လိုမျိုး အခုမှ အပြေးအလွှား အမှီလိုက်လေ့လာရာမှာ အထောက်အကူ ဖြစ်စေဖို့အတွက် ရည်ရွယ်ပြီး ဒီစာအုပ်ကို ရေးသားဖြစ်ခဲ့ပါတယ်။

ဒါပေမယ့် Bitcoin နဲ့ Cryptocurrency ဆိုတာ အခုချိန်မှာ နည်းပညာသမားတွေမှသာ စိတ်ဝင်စားတဲ့အရာ မဟုတ်ဘဲ၊ လူတိုင်းစိတ်ဝင်စားတဲ့ အရာတစ်ခု ဖြစ်နေပြီမို့လို့ နည်းပညာသမား မဟုတ်သူတွေပါ ဖတ်ရှု လေ့လာလို့ရအောင် ကြိုးစားရေးသားခဲ့ပါတယ်။ စာရေးသူ ရေးခဲ့ဖူးသမျှ စာအုပ်တွေထဲမှာ ကုဒ်တစ်လုံးမှ မပါတဲ့ ပထမဆုံး စာအုပ်တစ်အုပ်ပါ။ ဒီလိုကြိုးစားရေးသားထားတဲ့ ကြားထဲကပဲ ကျွမ်းကျင်ရာနောက်ခံ ကြောင့် နည်းပညာဆန်နေသေးလို့ တချို့အပိုင်းတွေ ဖတ်ရှုရ ခက်ခဲ ခဲ့မယ်ဆိုရင်လည်း နားလည်ခွင့်လွှတ် ပေးစေချင်ပါတယ်။

ဒီစာအုပ်ဟာ နည်းပညာသမားများ အတွက် Blockchain နည်းပညာတွေကို အမှီလိုက်ရာမှာ အထောက် အကူဖြစ်စေတဲ့ စာတစ်အုပ် ဖြစ်လိမ့်မယ်လို့ မျှော်လင့်ပါတယ်။ နည်းပညာသမား မဟုတ်တဲ့သူတွေအတွက် ဆိုရင်လည်း ရှုပ်ထွေးဆန်းကျယ်ပါတယ်ဆိုတဲ့ Bitcoin တို့ Cryptocurrency တို့လို အကြောင်းအရာတွေ ကို လိုတိုရှင်း နားလည်သဘောပေါက် သွားစေတဲ့ စာတစ်အုပ် ဖြစ်လိမ့်မယ်လို့ မျှော်လင့်ပါတယ်။

စာဖတ်သူများအားလုံးကို အထူးကျေးဇူးတင်ကြောင်း ပြောလိုပါတယ်။ အားလုံးပဲ ကိုယ်စိတ်နှစ်ဖြာ ကျန်းမာ ချမ်းသာပြီး၊ ရောဂါကပ်ဘေးများနဲ့ ရန်သူမျိုး (၅) ပါးတို့ရဲ့ ဘေးကနေ ကင်းဝေးနိုင်ကြပါစေ။

အိမောင် (Fairway)

၂၀၂၁ ခုနှစ်၊ ဇွန်လ (၂၉) ရက်နေ့တွင် ရေးသားပြီးစီးသည်။