សៀវភៅបង្ហាត់បង្រៀនកម្រិតមូលដ្ឋាន

Blockchain for Beginner

លោកគ្រូ សុខគីមហេង

២០២០

ប្លុកឆេនកម្រិតមូលដ្ឋាន

សេចក្តីផ្តើម

ប្លុកឆេន (Blockchain) គឺជាបច្ចេកវិទ្យាមួយដែលបានរកឃើញនៅឆ្នាំ២០០៨ ដើម្បីសម្រួលដល់ការទូទាត់លុយនៅលើអ៊ីនធឺណែតដោយងាយស្រួលនិងសុវត្ថិភាព។ ដោយសារមានការចាប់អារម្មណ៍ពីសំណាកអ្នកស្រាវជ្រាវ អ្នកពាណិជ្ជកម្មនិងសាធារណៈជន ហើយពុំមានឯកសារជាភាសាខ្មែរដើម្បីពន្យល់ពីបច្ចេកវិទ្យាមួយនេះ ទើបខ្ញុំចងក្រងសៀវភៅប្លុកឆេនកម្រិតមូលដ្ឋាន ដែលរៀបរាប់ខ្លីៗនិងមិនស៊ីជម្រៅ តែងាយក្នុងការអោយមីត្តអ្នកអានចាប់ផ្តើមយល់ដឹងពីបច្ចេកវិទ្យានេះ ដើម្បីជាទុនក្នុងការទៅបន្តសិក្សាបន្ថែមទៀតអោយកាន់តែស៊ីជម្រៅប្រសិនបើចាប់អារម្មណ៍។

មុននឹងឈ្វេងយល់ហេតុអ្វីមនុស្សបង្កើតបច្ចេកវិទ្យានេះឡើង យើងត្រូវសិក្សាពីប្រវត្តិសាស្ត្របន្តិចដោយសារតែបច្ចេកវិទ្យាមួយនេះ ពាក់ព័ន្ធជាមួយនឹងរឿងលុយមុនគេ យើងនឹងលើកយករឿងលុយមកពិភាក្សាបន្តិច។ កាលពីសម័យដើម មិនទាន់មានរូបិយបណ្ណ ប្រាក់រៀល ប្រាក់ដុល្លារ ការទូទាត់ទំនិញគឺធ្វើឡើងដោយការផ្លាស់ប្តូរគ្នា យកត្រីប្តូរអង្ករ យកអង្ករប្តូរគ្រឿងប្រើប្រាស់ ជាដើម។ ដោយការផ្លាស់ប្តូរបែបនេះមានការលំបាក មនុស្សចាប់ផ្តើមចេះប្រើប្រាស់វត្ថុផ្សេងៗ ដើម្បីរក្សាតម្លៃទុកសម្រាប់ធ្វើការផ្លាស់ប្តូរ ដូចជាគេប្រើ សំបកខ្យង គ្រាប់អង្កាំ ថ្មមានតម្លៃ ក្រោយមកយើងឃើញមាន លោហៈធាតុផ្សេងៗដូចជា សំរិទ្ធ ស្ពាន់ ប្រាក់ មាស ជាដើម។ ដោយសារលោហៈធ្ងន់ ហើយកម្រ ប្រទេសចិនបានផ្លាស់ប្តូររូបិយបណ្ណមកជាក្រដាសប្រាក់នៅចន្លោះសតវត្សទី៦និងទី៧ ក្នុងរជ្ជកាល ថាង។

ជាទូទៅ ប្រទេសនិមួយៗមានរូបិយបណ្ណរៀងៗខ្លួន ដូចជាកម្ពុជាប្រើប្រាក់រៀល សហរដ្ឋអាមេរិកប្រើប្រាក់ដុល្លារ ប្រទេសថៃប្រើប្រាក់បាត និង ប្រទេសវៀតណាមប្រើប្រាក់ឌុងជាដើម។ ដោយឡែកក្នុងសង្គមកម្ពុជា យើងឃើញមានការប្រើប្រាស់ប្រាក់ចំរុះ ដោយសារតែចង់បង្កភាពងាយស្រួលដល់ការទូទាត់ទំនិញ ដែលពេលខ្លះយើងក៏ភ្លេចអោយតម្លៃប្រាក់រៀល ទើបកាលពីឆ្នាំ២០១០ ខ្ញុំបានតែងសុភាសិត១០០០ឃ្លា ក្នុងឃ្លាទី៤មានសេចក្តីថា “***ប៉ោយប៉ែតជាយដែនប្រឹងចាយលុយបាត ស្វាយរៀងសង្វាតខំចាយលុយឌុង អ្នកមានចំណេះរស់នៅទីក្រុង ទិញគ្រឿងកំប៉ុងដកលុយដុល្លារ***” ពេលនោះគឺមានការចាប់អារម្មណ៍ និង មានការបំផុសស្មារតីស្រឡាញ់ប្រាក់រៀល រហូតមកដល់សព្វថ្ងៃយើងឃើញមាន ការបោះពុម្ពនិមិត្តសញ្ញាប្រាក់រៀលនៅលើមួក អាវយឺត ព្រមទាំងដាក់គំនាបដល់ហាងណា ក្រុមហ៊ុនណា ក្រសួងណាដែលមិនព្រមទទួលយកប្រាក់រៀលក្នុងការទូទាត់ សូម្បីធនាគារជាតិសព្វថ្ងៃ ក៏បានបង្កើតយុទ្ធនាការស្រឡាញ់ប្រាក់រៀលជាដើម។

ជាទូទៅ រូបិយបណ្ណជាតិត្រូវបានបោះពុម្ពដោយរដ្ឋ និង ក្រសួងពាក់ព័ន្ធក្រោមឱវាទ ហើយតែងតែមានតម្លៃលើវត្ថុមានតម្លៃ តួយ៉ាងដូចជាមាសជាដើម។ ដើម្បីទប់ស្កាត់ការបោះពុម្ពលុយតាមទំនើងចិត្ត ធ្វើអោយតម្លៃលុយធ្លាក់ចុះ អតិផរណាកើតឡើង តួយ៉ាងដូចជាប្រទេសហ្សីមបាវ៉ែ ដែលចាយលុយទាំងបាវៗ ដោយសារលុយគ្មានតម្លៃ។ អ្វីដែលគួរកត់សំគាល់ នៅខែសីហា ឆ្នាំ១៩៧១

ប្រធានាធិបតីសហរដ្ឋ អាមេរិក Richard Nixon បានប្រកាសលែងអោយមានការប្តូរប្រាក់ដុល្លារជាមួយនឹងមាសតទៅទៀតដើម្បីដោះស្រាយវិបត្តិសេដ្ឋកិច្ចរបស់ខ្លួន ព្រឹត្តិការណ៍នោះមានឈ្មោះថា Nixon Shock។

ហេតុផលទី១ ដែលបច្ចេកវិទ្យាប្តូរឆេន(Blockchain) ត្រូវបានបង្កើតឡើងរួមជាមួយលុយអេឡិចត្រូនិច (bitcoin) គឺដោយសារតែមនុស្សមួយក្រុមមិនចង់ផ្តល់អំណាចនៃការបោះពុម្ពលុយទៅលើរដ្ឋ ដោយសារការបោះពុម្ពគ្មានតម្លាភាពដែលអាចបង្ករជាវិបត្តិអតិផរណានៅក្នុងសង្គម។
ហេតុផលទី២ ពាក់ព័ន្ធជាមួយនឹងវិបត្តិសេដ្ឋកិច្ចកាលពីចន្លោះឆ្នាំ២០០៨ ដែលគេហៅថា Housing Bubble មួយផ្នែកនៃដើមហេតុនោះ គឺគេក៏បានចោទប្រកាន់ទៅលើធនាគារផងដែរ។
ហេតុផលទី៣ សម័យបច្ចេកវិទ្យា បានធ្វើអោយអ្វីៗគ្រប់យ៉ាងប្រែក្លាយជាឌីជីថល ឬ អេឡិចត្រូនិច ការបង្កើតលុយអេឡិចត្រូនិចមិនមែនទើបកើតឡើងនៅឆ្នាំ២០០៨នោះទេ គឺកើតតាំងពីយូរណាស់មកហើយ ការចាយលុយតាមកាតATM (VISA Card, Master Card) ក៏ចាត់ទុកជាការចាយលុយបែបអេឡិចត្រូនិច។ ដោយឡែកនៅឆ្នាំ២០០៨ គឺបានបង្កើតរូបិយបណ្ណថ្មី ដែលមិននៅក្រោមការគ្រប់គ្រងរបស់រដ្ឋ ដោយប្រើប្រាស់បច្ចេកវិទ្យា Cryptography និង Blockchain ទើបរូបិយបណ្ណថ្មីនោះគេហៅថា Cryptocurrency = Cryptography + Currency លុយគ្រីពតូ ឬ លុយអេឡិចត្រូនិច។

១ BITCOIN លុយគ្រីពតូដំបូង

ការបង្កើតលុយគ្រីពតូដំបូងដែលជោគជ័យ

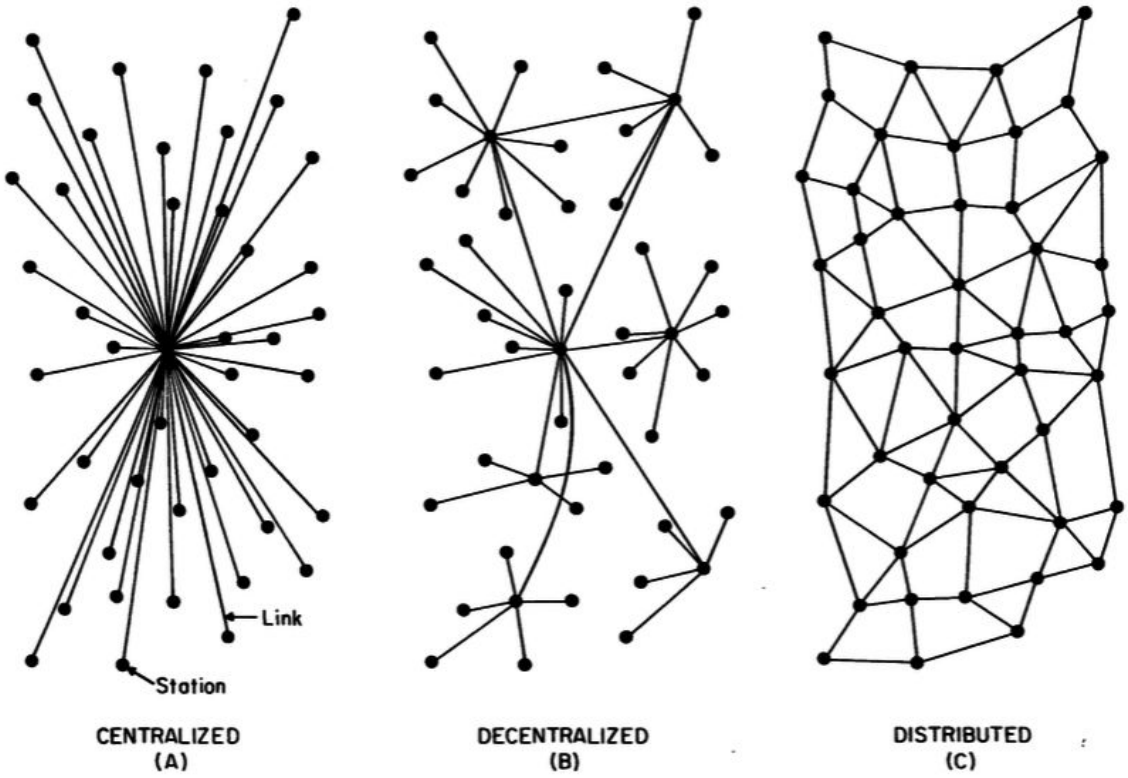
អ្នកស្រាវជ្រាវជាច្រើនបានបង្កើតលុយអេឡិចត្រូនិច តែមិនទទួលបានជោគជ័យដោយសារពួកគេមិនអាចដោះស្រាយបញ្ហាមួយបាន នៅពេលដែលលុយក្រដាសក្លាយជាលុយអេឡិចត្រូនិចដែលភាសាបច្ចេកទេសហៅថា Double Spending Problem ឬ Infinit Spending Problem។ មានន័យថាលុយតូលេខនៅលើអ៊ីនធឺណែត យើងអាចCopy Paste បាន តើត្រូវធ្វើដូចម្តេចដើម្បីកុំអោយមនុស្សម្នាក់ចាយលុយដដែល លើសពីម្តង។ រត្តមាននៃការបង្កើតលុយអេឡិចត្រូនិចមានតាំងពីឆ្នាំ១៩៨២រហូតមក មានដូចជា E-Cash, Hash-Cash, B-Money,Bit-Gold ក៏ប៉ុន្តែប្រព័ន្ធទាំងអស់នោះ នៅតែមិនអាចដោះស្រាយបញ្ហា Double Spending Problem នៅក្នុង Distributed System បាន។

នៅឆ្នាំ២០០៨ មានជនអនាមិក ដែលគេមិនបានស្គាល់ថា ជាប្រុសឬស្រី ជនជាតិអ្វី ជាបុគ្គលម្នាក់ឬជាក្រុមដែលបានដាក់រហ័សនាមថា Satoshi Nakamoto បានសរសេរអត្ថបទស្រាវជ្រាវមួយ

បកស្រាយពីការដោះស្រាយបញ្ហាខាងលើ ដែលអត្ថបទនោះមានចំណងជើងថា “Bitcoin: A Peer-to-Peer Electronic Cash System” ដែលបានជ្រើសរើសបច្ចេកទេសដែលអ្នកស្រាវជ្រាវមុនៗបានរក ឃើញ គួបផ្សំនឹងគំនិតច្នៃប្រឌិត បង្កើតបានជាប្រព័ន្ធទូទាត់លុយអេឡិចត្រូនិចដំបូងមួយ
ដែលអាចដោះស្រាយបញ្ហាដែលអ្នកស្រាវជ្រាវមុនៗមិនអាចដោះស្រាយបាន ព្រមទាំងបានបង្កើតរូបិយបណ្ណថ្មីមួយមានឈ្មោះថា bitcoin។ គេមិនទាន់ហៅបច្ចេកវិទ្យានោះថា ប្លុកឆេន (Blockchain) នៅឡើយទេ នៅក្នុងអត្ថបទនោះបានពន្យល់ពីរចនាសម្ព័ន្ធនៃការរក្សាទិន្នន័យ ប្រតិបត្តិការលុយជាលក្ខណៈ Block ដែលហៅថា Chain of Blocks ក្រោយមកដើម្បីងាយស្រួលហៅ ទើបគេប្តូរមកហៅថា Blockchain រហូតមកដល់សព្វថ្ងៃ។

៤ Centralization, Decentralization, Distributed

បច្ចេកវិទ្យាប្លុកឆេន អាចចាត់ទុកថាជាបច្ចេកវិទ្យា Distributed Ledger Technology (DLT) ដែលបានរក្សា
ប្រតិបត្តការនៃការទូទាត់លុយជាលក្ខណៈបែងចែករាយប៉ាយនៅច្រើនម៉ាស៊ីនកុំព្យូទ័រផ្សេងៗគ្នា។
ដើម្បីយល់ច្បាស់ពីប្រព័ន្ធនេះ យើងនឹងសិក្សាពីភាពខុសគ្នានៃប្រព័ន្ធ៣យ៉ាងដូចខាងក្រោម:



Centralization System

គឺជាប្រព័ន្ធគ្រប់គ្រងប្រមូលផ្តុំ មានអ្នកគ្រប់គ្រងឬអ្នកសម្រេចចិត្តតែម្នាក់ អាចធ្វើការផ្លាស់ប្តូរច្បាប់នានាបានដោយអត្តនោម័ត មិនចាំបាច់រងចាំយោបល់ពីអ្នកដទៃ។

គុណសម្បត្តិ

ងាយស្រួលតម្លើង ងាយស្រួលគ្រប់គ្រង ងាយស្រួលកែប្រែ ល្បឿនប្រតិបត្តិការលឿន ចំណាយថវិការលើឧបករណ៍តិច។

គុណវិបត្តិ

ប្រព័ន្ធការពារសន្តិសុខ មានចំនុចខ្សោយមួយដែលអ្នកបច្ចេកទេសហៅថា Single Point of Failure។ ដើម្បីធ្វើអោយប្រព័ន្ធមិនដំណើរការ ឬ មានបញ្ហា គ្រាន់តែធ្វើអោយ Server នោះមានបញ្ហា ឬ ប្រើប្រាស់គណនី Administrator អាចធ្វើអោយប្រព័ន្ធទាំងមូលប្រើការលែងបាន ឬ ទិន្នន័យត្រូវបានកែប្រែ។ ក្រៅពីបញ្ហាបច្ចេកទេស គឺបញ្ហាគ្រប់គ្រងនិងការសម្រេចចិត្ត គឺផ្អែកលើបុគ្គលម្នាក់ដែលមានសិទ្ធិធំជាងគេ អាចធ្វើអ្វីៗគ្រប់បែបយ៉ាងបាន។

Decentralization System

ដោយសារតែមានគុណវិបត្តិនៃប្រព័ន្ធខាងលើ គេបានបន្ថែមម៉ាស៊ីនមេ (Server) ២ ឬច្រើនដាក់នៅកន្លែងខុសគ្នា ប្រសិនបើមួយមិនដំណើរការ គឺនៅសល់មួយទៀត។ ការគ្រប់គ្រងមានភាពលំបាកជាងមុនបន្តិច តែប្រព័ន្ធការពារសន្តិសុខក៏បានខ្លាំងជាងមុនបន្តិចដូចគ្នា ក៏ប៉ុន្តែនៅតែមិនទាន់ដោះស្រាយបញ្ហាខាងលើបានដដែរ។

Distributed System

គឺជាប្រព័ន្ធដែលគ្មានមេគ្មានកូន (No Master - Slave) កុំព្យូទ័រទាំងអស់មានសិទ្ធិស្មើៗគ្នា ធ្វើការដូចគ្នា រក្សាទិន្នន័យដូចគ្នា នៅពេលដែលមានម៉ាស៊ីនមួយមានបញ្ហា នៅមានម៉ាស៊ីនជាច្រើនទៀតនៅដំណើរការធម្មតា ធានាបាននូវសេវាកម្ម 24/7។

គុណសម្បត្តិ

ប្រព័ន្ធការពារខ្លាំងជាងមុន ទិន្នន័យមិនអាចកែប្រែតាមចិត្ត មិននៅក្រោមការគ្រប់គ្រងរបស់បុគ្គលម្នាក់។

គុណវិបត្តិ

ចំណាយថវិការច្រើនជាងមុនលើឧបករណ៍ ការគ្រប់គ្រងពិបាកជាងមុន ល្បឿនប្រតិបត្តិការយឺតជាងមុន ត្រូវការធនធានមនុស្ស និង កែប្រែរបៀបនៃការធ្វើការនិងការសម្រេចចិត្ត។

ប្លុកឆេន Bitcoin គឺជាប្រព័ន្ធ Distributed System ឬ ហៅថា Peer-to-Peer System។ ក្នុងចំណោមប្រព័ន្ធទាំង៣ដែលបានបកស្រាយខាងលើ ពុំមានប្រព័ន្ធណាល្អជាងប្រព័ន្ធណាឡើយ ប្រព័ន្ធមួយៗសុទ្ធតែមានចំនុចខ្លាំងនិងខ្សោយរៀងៗខ្លួន អាស្រ័យទៅនឹងតម្រូវការរបស់អ្នកប្រើប្រាស់ថា ពាណិជ្ជកម្មរបស់យើងសាកសមជាមួយប្រព័ន្ធមួយណាជាង ឬ ពេលខ្លះគេអាចបង្កើតប្រព័ន្ធចំរុះ (Hybrid System) ដែលមានផ្នែកខ្លះ Centralized និង ផ្នែកខ្លះទៀត Distributed។

៣ ភាពខុសគ្នានៃគណនីធនាគារ និង គណនីប្លុកឆេន

	ធនាគារ	ប្លុកឆេន (bitcoin)
ការបង្កើតគណនី	ទាមទារអត្តសញ្ញាណម្ចាស់គណនី • អត្តសញ្ញាណប័ណ្ណ • រូបថត	មិនទាមទារអត្តសញ្ញាណ • អនាមិក (Anonymous)
លេខគណនី	បង្កើតដោយធនាគារ មានទម្រង់ជាលេខ	ប្រើប្រាស់កម្មវិធីបង្កើត Account Address ចេញពី Public Key មានទម្រង់ជាលេខនិងអក្សរច្រើនខ្ទង់
លេខសំងាត់	លេខកូដ៤ទៅ៦ខ្ទង់	Private Key មានទម្រង់ជាលេខនិងអក្សរច្រើនខ្ទង់
ការបូបលុយ និង ការចាយលុយ	អាចចាយតាមកាតATM ឬដកជាក្រដាសប្រាក់ទុកក្នុងការបូបលុយ	ប្រើប្រាស់កម្មវិធី Wallet Software ដែលផ្ទុក Account Address និង Private Key ហើយចាយតាមSoftwareនោះ
រូបិយបណ្ណ	សំគាល់តាមប្រទេសនីមួយៗ មានរដ្ឋទទួលស្គាល់ស្របច្បាប់ ឧ. ប្រាក់រៀល	តាមការនិយមនៃអ្នកប្រើប្រាស់ ស្របច្បាប់និងមិនស្របច្បាប់ដោយកន្លែង ឧ. bitcoin
ការរក្សាទិន្នន័យ	នៅលើServerរបស់ធនាគារ	នៅតាមកុំព្យូទ័រឯកជនរបស់អ្នកប្រើប្រាស់ទូទៅដែលហៅថា Miner (ម៉ាស៊ីនជីករ៉ែ) ច្រើនកន្លែង
ការបោះពុម្ពលុយ	រដ្ឋ និង ក្រសួងក្រោមឱវាទ	ច្បាប់ដែលបានចងក្រងក្នុងប្លុកដំបូង ដែលហៅថា Genesis Block បង្កើតដោយស្ថាបនិកប្លុកឆេននិមួយៗ ក្នុងករណីbitcoin គឺ Satoshi Nakamoto
តម្លៃលុយ	ធៀបនឹងសេដ្ឋកិច្ច តម្លាភាព និង ទំនុកចិត្តនៃរដ្ឋបាលនីមួយៗ	ធៀបនឹងតម្រូវការនិងការផ្គត់ផ្គង់ ដោយមានប្រព័ន្ធ Cryptocurrency Ecosystem ដែលបានបង្កើតឡើងដោយ Founder, Investor និង Adopter (ស្ថាបនិក អ្នកវិនិយោគ អ្នកគាំទ្រ)
ការសម្រេចចិត្ត	រដ្ឋ និង ក្រសួងក្រោមឱវាទ	ស្ថាបនិក ក្រុមអ្នកបង្កើតកម្មវិធី អ្នកវិនិយោគ មតិភាគច្រើននៃអ្នកប្រើប្រាស់

៤ ប្លុកឆេនសាធារណៈ និង ឯកជន

បច្ចេកវិទ្យាប្លុកឆេនកើតឡើងតាំងពីឆ្នាំ២០០៨ រហូតមកដល់ពេលនេះ មានអាយុកាល១២ឆ្នាំហើយ នោះមានន័យថា មានការវិវត្តន៍ និង កែប្រែ ព្រមទាំងមានប្រភេទប្លុកឆេនខុសៗគ្នាជាច្រើន ដែលបង្កើតឡើងដោយក្រុមហ៊ុន ធនាគារជាច្រើនប្លែកៗពីគ្នា។ ប្រសិនបើយើងហៅប្រព័ន្ធមួយថាប្លុកឆេន វាមិនទាន់បញ្ជាក់អំពីហេដ្ឋារចនាសម្ព័ន្ធ ច្បាប់ ការគ្រប់គ្រង បច្ចេកវិទ្យាដែលនៅពីក្រោយប្លុកឆេននោះឡើយ។ ខាងក្រោមនេះ យើងនឹងរៀបរាប់ពីប្រភេទប្លុកឆេនទាំងនោះ:

Public Blockchain / Permissionless Blockchain

គឺជាប្រភេទប្លុកឆេនសាធារណៈ ដែលអ្នកណាក៏អាចចូលរួមបាន ហើយមិនតម្រូវអោយបង្ហាញអត្តសញ្ញាណ ប្រៀបដូចជា Bitcoin Blockchain ឬ Ethereum Blockchain ជាដើម។ រាល់ការសម្រេចចិត្តផ្អែកទៅលើមតិភាគច្រើន ក៏ប៉ុន្តែនៅពេលដែលសហគមន៍សាធារណៈនេះកាន់តែធំទៅៗ ហើយពេលណាមួយនោះ មានការខ្វែងគំនិតគ្នា គេនឹងចាប់ផ្តើមហែក Blockchain ជា២ ជា៣ ជា៤ បន្តបន្ទាប់ ដើម្បីធ្វើការកំណត់ច្បាប់រៀងៗខ្លួនទៅតាមសហគមន៍តូចៗរបស់គេ ដែលព្រឹត្តិការណ៍នោះហៅថា Blockchain Fork។

Private Blockchain / Permissioned Blockchain

គឺជាប្រភេទប្លុកឆេនឯកជន ជាកម្មសិទ្ធរបស់ធនាគារមួយ ឬ ក្រុមហ៊ុនសម្ព័ន្ធមួយក្រុម ដែលអ្នកចូលរួមមានអត្តសញ្ញាណច្បាស់លាស់ មិនអនុញ្ញាតិអោយសាធារណជនចូលរួមដោយសេរី គេច្រើនប្រើប្រាស់ប្លុកឆេនបែបនេះ សម្រាប់សហគ្រាសឯកជន។ ឧទាហរណ៍ ដូចជា Hyperledger ដែលជាប្លុកឆេនប្រភេទ Permissioned និង Opensource។

Cryptocurrency and SCAM Blockchain

ដោយសារតែបច្ចេកវិទ្យាប្លុកឆេនកើតឡើង ទន្ទឹមគ្នាជាមួយលុយគ្រីពតូ ឬ លុយអេឡិចត្រូនិច មានក្រុមហ៊ុនជាច្រើន បានបង្កើតលុយគ្រីពតូជាច្រើន ខ្លះក៏ប្រើបច្ចេកវិទ្យាប្លុកឆេនត្រឹមត្រូវ ខ្លះទៀតក៏ប្រើប្រព័ន្ធគ្រប់គ្រងទិន្នន័យធម្មតាដូចជា Database ដើម្បីបង្កើតលុយអេឡិចត្រូនិចថ្មីៗដើម្បីបោកបញ្ឆោទអ្នកវិនិយោគជើងថ្មី ខ្លះរស់បានយូរឆ្នាំ ខ្លះក៏ឆាប់ដួលទៅវិញ ហើយខ្លះទៀតប្រមូលលុយហើយរត់បាត់ ដែលប្លុកឆេនទាំងនោះ ចាត់ទុកជាប្លុកឆេនដែលគ្មានប្រយោជន៍ ឬ ប្លុកឆេនបោកប្រាស់។

ហានិភ័យ Risk និង ការវិនិយោគ Investment ជាមិត្តនឹងគ្នា អ្នកចង់វិនិយោគត្រូវស្គាល់ ចេះគ្រប់គ្រង និង ចេះកាត់បន្ថយហានិភ័យ បើមិនដូច្នោះទេ អ្នកនឹងក្លាយជាទាសករនៃការវិនិយោគ។

៥ បច្ចេកទេសប្លុកឆេន

ពាក្យបច្ចេកទេស

Block ប្លុក កន្លែងរក្សាទិន្នន័យនៃប្រតិបត្តិការជាច្រើន ដែលបានចងក្រងជាប្លុកមានទំហំ ជាក់លាក់

Blockchain ប្លុកឆេន ប្លុកដែលភ្ជាប់គ្នាជាសង្វាក់ យើងហៅថាខ្សែសង្វាក់ប្លុកឆេន ដោយប្លុកកើតថ្មីត្រូវភ្ជាប់ជាមួយប្លុកមុន។

Genesis Block គឺជាប្លុកដែលកើតដំបូងគេបង្អស់ហើយពុំមានភ្ជាប់ទៅកាន់ប្លុកមុនណាទៀត រាល់ក្បួនច្បាប់នានាគឺបានកត់ត្រាក្នុងប្លុកមួយនេះ។

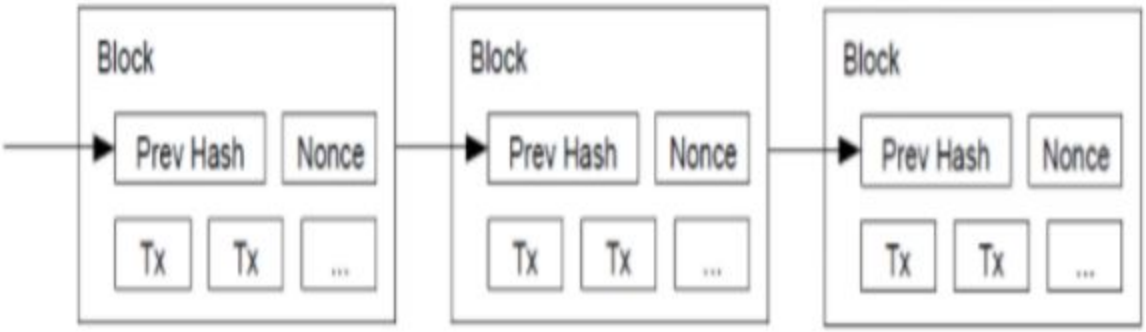
Ledger បញ្ជីកំណត់ត្រា ជាបញ្ជីដែលបានកត់ត្រារាល់ប្រតិបត្តិការនៃការទូទាត់ទាំងអស់។

Transaction ប្រតិបត្តិការ គឺជាការធ្វើប្រតិបត្តិការមួយ ក្នុងករណីលុយ គឺការផ្ទេរលុយទៅវិញទៅមក។

Transaction Fee ថ្លៃសេវា រាល់ការធ្វើប្រតិបត្តិតែងមានកុំព្យូទ័រមួយប្រភេទដែលយើងហៅថា Miner សម្រាប់ធ្វើការកត់ត្រា និង ត្រួតពិនិត្យប្រតិបត្តការនោះ ហេតុដូច្នេះ គឺយើងត្រូវបង់ថ្លៃសេវាមួយចំនួនរាល់ប្រតិបត្តិការនានា។

Miner ម៉ាស៊ីនជីករ៉ែ ក្នុងន័យនេះមិនមែនជាម៉ាស៊ីនដែលជីករ៉ែក្នុងដីនោះទេ គឺជាប្រភេទម៉ាស៊ីនដែលធ្វើការរុករកចម្លើយនៃរូបមន្តគណិតវិទ្យាដែលយើងហៅថាតម្លៃHash ដើម្បីបង្កើតប្លុកថ្មីៗ។

Mining ការជីករ៉ែ សកម្មភាពនៃការគណនាតម្លៃHashនោះ យើងហៅថាការជីករ៉ែ។



ដំណើរការចាយលុយតាមប្លុកឆេន

1. បង្កើតកាបូបលុយមួយ យើងអាចបង្កើតដោយខ្លួនឯង ឧទាហរណ៍ គេហទំព័រ bitaddress.org អាចអោយយើងបង្កើតកាបូបលុយ bitcoin បាន។ ត្រូវចាំថា ក្នុងកាបូបលុយគឺមាន Account Address និង Private Key បើនរណាគេម្នាក់មាន Private Key របស់យើងនោះមានន័យថាគេអាចចាយលុយយើងបាន។ ការបង្កើតកាបូបលុយដោយប្រើគេហទំព័រមួយដែលយើងមិនស្គាល់ ឬ ប្រើប្រាស់កម្មវិធីកាបូបលុយ (Wallet Software) ពីក្រុមហ៊ុនដែលយើង

មិនស្គាល់ នៅពេលដែលយើងបញ្ចូលលុយចូលក្នុងកាបូបលុយនោះ ក្រុមហ៊ុននោះអាចនឹងដកលុយយើងចាយបាន ប្រសិនបើគេមាន Private Key របស់យើង

2. កាបូបលុយដែលបង្កើតហើយគឺពុំមានលុយទេ នោះត្រាតែត្រូវបានអ្នកដែលធ្លាប់មានលុយ ហើយធ្វើប្រតិបត្តិការផ្ទេរលុយមកអោយយើង ជាទូទៅលុយគ្រីពតូដំបូងគឺកើតពីខ្យល់ ពីការជុប ហើយទើបត្រូវបានផ្ទេរពីមនុស្សម្នាក់ៗមនុស្សម្នាក់ទៀត តាមរយៈការធ្វើប្រតិបត្តិការ (Transaction) មានវិធីជាច្រើនដើម្បីទទួលបានលុយគ្រីពតូ គឺទៅទិញពីអ្នកដែលមាន ទៅទិញពីទីផ្សារអនឡាយ ឬ ទៅទិញពីម៉ាស៊ីន ពេលនោះម៉ាស៊ីនឬបុគ្គលឬក្រុមហ៊ុនដែលយើងយកលុយក្រដាសទៅទិញ នឹងផ្ញើលុយគ្រីពតូចូលកាបូបលុយអេឡិចត្រូនិចរបស់យើង
3. លុយគ្រីពតូមិនទាន់ជាលុយដែលគេទទួលស្គាល់ទូលំទូលាយនោះទេ ដូចនេះការចាយលុយគឺលុះតែមានការឯកភាព រវាងអ្នកទិញ និង អ្នកលក់ដែលមានកាបូបលុយដូចគ្នា ហើយប្រើប្រាស់កម្មវិធីកាបូបលុយនោះ ដើម្បីផ្ទេរលុយអោយគ្នាទៅវិញទៅមក ប្តូរជាមួយទំនិញ ឬ សេវាកម្មដែលទទួលបាន
4. នៅពេលដែលអ្នកប្រើប្រាស់ណាម្នាក់ធ្វើការផ្ទេរលុយ ប្រតិបត្តិការនោះនឹងបញ្ចូនពីកម្មវិធីកាបូបលុយទៅកាន់ម៉ាស៊ីនជីករ៉ែ ម៉ាស៊ីនជីករ៉ែទាំងអស់ប្រមូលយកប្រតិបត្តិការនាំនាដែលមិនទាន់បានត្រួតពិនិត្យ និង មិនទាន់បានកត់ត្រាក្នុងប្លុកឆេន យកមកពិនិត្យ ហើយចងក្រងជាប្លុកមួយដែលមានទំហំជាក់លាក់ រួចធ្វើសកម្មភាពជីករ៉ែ ដោយការស្វែងរកលេខមួយដែលហៅថា Nonce ដែលលេខនោះជាចម្លើយដែល អាចបង្កើតជាតម្លៃHash សម្រាប់ទៅបង្កើតជា ID នៃប្លុកថ្មីមួយ ម៉ាស៊ីនជីករ៉ែណាដែលបានរកឃើញតម្លៃNonceនោះមុនគេ ស្របទៅតាមរូបមន្តដែលបានកំណត់ ម៉ាស៊ីនជីករ៉ែនោះនឹងទទួលបានរង្វាន់ (Reward) ជាលុយគ្រីពតូពីប្រព័ន្ធប្លុកឆេន ព្រមទាំងថ្លៃសេវា (Transaction Fee)ទាំងអស់ ពីប្រតិបត្តិការនិមួយៗ ការផ្តល់រង្វាន់បែប នេះទើបធ្វើអោយប្រព័ន្ធប្លុកឆេនដំណើរការទៅមុខបាន
5. ការរុករកតួលេខNonce ដែលយើងហៅថាការជីករ៉ែ (Mining) នោះគឺដើម្បីរកចម្លើយដែលម៉ាស៊ីនទាំងអស់ត្រូវឯកភាពគ្នាលើរូបមន្តរួមមួយ ដែលក្បួនច្បាប់នេះ យើងហៅថា Consensus Algorithm ច្បាប់នៃការឯកភាព ដែលនៅក្នុងប្លុកឆេនមានឈ្មោះជាក់លាក់មួយ ហៅថា Proof of Work (PoW) Consensus Algorithm។

ការបង្កើតលេខគណនី Account Address

លេខគណនីរបស់ប្លុកឆេនBitcoin គឺកើតចេញពី Public Key ហើយ Public Key គឺកើតចេញពី Private Key។ នោះមានន័យថាដំបូងយើងត្រូវបង្កើត Private Keyជាមុនសិន Private Key មានទំហំស្មើនឹង 256 bits ឬ 32 Bytes បើគេសរសេរជាទំរង់ Hexadecimal ប្រព័ន្ធគោល១៦ នោះ Private Key នឹងមានចំនួន 64 ខ្ទង់ជាលេខ0ដល់9 និង Aដល់F។

ឧទាហរណ៍យើងមាន Private Key ដូចខាងក្រោម
0xA0DC65FFCA799873CBEA0AC274015B9526505DAAAED385155425F70810198421

Public Key គឺជាចំនុចនៅលើខ្សែកោង Elliptic Curve ដែលប្លុកឆេនBitcoin ប្រើប្រាស់ខ្សែកោង Secp256k1 ដើម្បីបង្កើត Public Private Key។ តាមរូបមន្តនៃខ្សែកោងនោះ យើងនឹងទទួលបានចំនុច(x,y) ចេញពី Private Key ដូចខាងក្រោម:

x=901015FB4072DE06225D029B97B2B7C2B55AF241A21CA63252C6136DFF650D41
y=E53F22D2C8F68A95FA879DFC54DEDEC27B7E3FA5D59C13749901885D4B1C9A20

យើងគ្រាន់តែបន្ថែមលេខ 04 ពីមុខចំនុចx y យើងនឹងទទួលបាន Public Key ដែលមានទំរង់ជា 04xy ដែលអាចយកទៅប្រើការបាន។

Public Key
04901015FB4072DE06225D029B97B2B7C2B55AF241A21CA63252C6136DFF650D41E53F22D2C8F68A95FA879DFC54DEDEC27B7E3FA5D59C13749901885D4B1C9A20

យើងក៏អាចសរសេរ Public Key ជាលក្ខណៈបង្រួម ដោយដាក់លេខ02នៅពីមុខប្រសិនបើ y ជាចំនុចគូ ហើយលុបតួលេខ y ចេញ។

Public Key
02901015FB4072DE06225D029B97B2B7C2B55AF241A21CA63252C6136DFF650D41

ឥឡូវនេះ គឺយើងមាន Private Key និង Public Key ហើយក៏ប៉ុន្តែលេខគណនីគឺមិនយក Public Key ទេ គឺគេមានវិធីបង្កើតលេខគណនីចេញពី Public Key ដោយHashជាមួយនឹង SHA256 បន្ទាប់មកយកទៅHashជាមួយនឹងRIPEMD160 ដែលវិធីសាស្ត្រនេះហៅថា Double Hashing។ បន្ទាប់យកគេយកលទ្ធផលដែលទទួលបានទៅបន្ថែម Network byte ពីខាងមុខ និងបន្ថែម Checksum ដែលជាលទ្ធផលពី Double Hashing ម្តងទៀតរួចយក 4 bytes ខាងដើមនៃលទ្ធផល ទៅបន្តជាមួយលទ្ធផលមុនចុងបញ្ចប់គឺគេធ្វើការបំលែងលទ្ធផលចុងក្រោយជាទំរង់ Base58Check ដែលយើងនឹងទទួលបានលេខគណនី Account Address ដែលអាចយកទៅប្រើការបាន។

លទ្ធផលក្រោយយក Public Key ទៅHashក្នុង Function SHA256
B72E8BBEF645323773B3B83AF6890FEC368E4611F8F075BB81EA361A8D2CDEE8

យកលទ្ធផលខាងលើទៅ Hash ម្តងទៀតជាមួយនឹង Function RIPEMD160
F7692AFC0E6CA9180BFD27AD6DEA9A84BD77AFB2

បន្ថែម Network Byte 0x00 នៅខាងមុខ
00F7692AFC0E6CA9180BFD27AD6DEA9A84BD77AFB2

បន្ថែម Checksum ដោយធ្វើការ Hash ពីរដងនៃលទ្ធផលខាងលើជាមួយនឹង Function SHA256
1st SHA256:
A6786491F36CD9B3FC19DA6C896BBA98909E5CB8F6A35A7D4721EA8F30CDB6E8

2nd SHA256:
666F5D67FCCDE933AECD6E39ADF1B7053C5AF0D56686A30D86227C3E6541D15C

ជ្រើសរើសយកលេខ 4 Bytesខាងមុខដែលស្មើនឹង8ខ្ទង់ធ្វើជា checksum
666F5D67

បន្ថែមChecksum នៅពីក្រោយលទ្ធផលមុន
00F7692AFC0E6CA9180BFD27AD6DEA9A84BD77AFB2666F5D67

បំលែងលទ្ធផលចុងក្រោយជាមួយ Base58Check Encoding យើងនឹងទទួលបាន Account Address
1PZBtaSN55GPaeA1u14FwzcCWhQkyyGs6e

ច្បាប់ឯកភាព Consensus Algorithm

ប្លុកឆេនBitcoin ប្រើប្រាស់ច្បាប់ឯកភាពមួយដែលមានឈ្មោះថា Proof of Work។ ដើម្បីបង្កើតប្លុកថ្មីមួយបានម៉ាស៊ីនជីករ៉ែទាំងអស់ត្រូវប្រមូលប្រតិបត្តិការមកចងក្រងជាប្លុក បូកជាមួយនឹងលេខមួយដែលហៅថា Nonce ដើម្បីស្វែងរកតម្លៃHash ដែលត្រូវតាមរូបមន្ត Target Difficulty (Bits) ដែលបានកំណត់ ទើបអាចបញ្ចូលប្លុកថ្មីនោះភ្ជាប់ទៅកាន់ប្លុកឆេន ហើយម៉ាស៊ីនជីករ៉ែណាដែលបានរកឃើញចម្លើយនៃលេខ Nonce ដែលត្រឹមត្រូវនឹងទទួលបានរង្វាន់ជាលុយគ្រីពតូពីប្លុកឆេនBitcoin។

ប្លុកឆេនបានបង្កើតច្បាប់មួយចំនួនដូចខាងក្រោម:

- ការផ្គត់ផ្គង់លុយគ្រីពតូសរុបគឺមានចំនួន ២១លានកាក់ (bitcoin)
- រយៈប្រហែល១០នាទី ទើបមានប្លុកថ្មីមួយកើតឡើង (រយៈពេលនេះអាចប្រែប្រួលបន្តិចបន្តួចអាស្រ័យនឹងលទ្ធភាពនៃការរកចម្លើយរបស់ម៉ាស៊ីនជីករ៉ែ)

- ម៉ាស៊ីនជីករ៉ែដែលបានរកចម្លើយឃើញនឹងទទួលបានប្រាក់រង្វាន់ ៥០ bitcoins ដែលប្រាក់រង្វាន់នេះ នឹងថយចុះពាក់កណ្តាលរាល់ ២១០,០០០ប្លុក ដែលប្រហែលជា៤ឆ្នាំម្តងគឺប្រាក់រង្វាន់នឹងថយចុះពី៥០ទៅ២៥ , ១២.៥, ៦.២៥, ៣.១២៥ រហូត ដល់លែងមានរង្វាន់ប្រគល់អោយអ្នកជីករ៉ែ
- រយៈពេល២សប្តាហ៍ ស្មើនឹង ២*៧*២៤*៦០ = ២០១៦០នាទី ស្មើនឹង២០១៦ប្លុក ការកំណត់ភាពលំបាកនៃការគណនាត្រូវបានកែប្រែ អោយស្រួលជាងមុន ឬ ពិបាកជាងមុន ផ្អែកទៅលើលទ្ធផល២សប្តាហ៍កន្លងទៅ
- ដើម្បីយល់ពីដំណើរការជីករ៉ែ ដំបូងយើងត្រូវស្គាល់រូបមន្តមួយដែលហៅថា Target Difficulty ឬ Bits ដែលសរសេរកាត់ជាលេខ៨ខ្ទង់ ឧទាហរណ៍ Bits = 180130E0 (18ជាExponent និង 0130E0ជា Coefficient) ដើម្បីសរសេរជាប្រព័ន្ធគោល១០ គេយក
  Coefficient * 2 ^ (8*(exponent-3)) =
  29201223626342991605750065618903157022235193117232857088
  យើងអាចសរសេរជាប្រព័ន្ធគោល១៦
  00000000000000000130e0000000000000000000000000000000000000000000
- តួនាទីរបស់អ្នកជីករ៉ែ គឺត្រូវយកប្រតិបត្តិការទាំងអស់ បូកជាមួយនឹងលេខNonce ដែលតូចជាង Target Difficult ដែលបានកំណត់ខាងលើ ដោយប្រើ Hash Function ។ ជាទូទៅ Hash Function គឺជារូបមន្តដែលយកធាតុចូលហើយបង្កើតជាលទ្ធផលដែលមានទំហំជាក់លាក់គឺ 256bits ឬ 64ខ្ទង់ ក៏ប៉ុន្តែគឺមិនងាយនឹងទទួលបានលេខសូន្យបន្តគ្នាជាច្រើនដូច Target Difficult ដែលបានកំណត់នោះទេ ចំនួនសូន្យពីមុខកាន់តែច្រើន ចំណាយពេលរកចម្លើយកាន់តែយូរ ហេតុដូច្នេះហើយ ម៉ាស៊ីនជីករ៉ែ ត្រូវប្តូរតួលេខ Nonce ពី 0,1,2,3,4 .....,1000, 1001, 1002, ...6453, 6454 រហូតលុះត្រាតែរកចម្លើយឃើញ ការធ្វើបែបនេះគឺហៅថាការជីករ៉ែ Minining។
- ដើម្បីរកចម្លើយនេះ ម៉ាស៊ីនជីករ៉ែត្រូវបានសមត្ថភាពក្នុងការគណនា ដោយគេប្រើប្រាស់ CPU ហើយម៉ាស៊ីនទាំងនោះកាន់តែវិវត្តន៍លឿនទៅៗ មានការប្រកួតប្រជែងច្រើន ហើយម៉ាស៊ីនថ្មីៗ ដែលមានល្បឿនកាន់តែលឿនត្រូវបានបង្កើតឡើង ដូចជា GPU, FPGA, ASIC ដែលធ្វើអោយការកំណត់កម្រិតនៃភាពលំបាកកាន់តែខ្ពស់ ចំណាយពេលយូរ និង ប្រើប្រាស់ថាមពលអគ្គីសនីច្រើន មូលហេតុនេះហើយទើបមាន ច្បាប់ឯកភាពថ្មីៗបានបង្កើតបន្ថែមទៀត ក្រៅពី Proof of Work (PoW) យើងឃើញមាន Proof of Stake (PoS) , Delegate Proof of Stake (DPoS) ជាដើម។

សេចក្តីបញ្ចប់

ដូចដែលបានរៀបរាប់ខាងលើ បច្ចេកវិទ្យាប្លុកឆេនត្រូវបានបង្កើតឡើងអស់រយៈ១២ឆ្នាំមកហើយ នោះមានន័យថា មានការកែប្រែ ក្បួនច្បាប់ បច្ចេកវិទ្យា មុខងារបន្ថែម រចនាសម្ព័ន្ធ របៀបរក្សាទិន្នន័យ របៀបទំនាក់ទំនង ច្បាប់ឯកភាព សន្តិសុខបច្ចេកវិទ្យា ខុសៗគ្នាទៅតាមប្លុកឆេននីមួយៗ ដែលបង្កើតឡើងដោយក្រុមហ៊ុន ឬ ស្ថាបននានា ហេតុដូចនេះ ដើម្បីយល់ដឹងពីបច្ចេកវិទ្យាមួយនេះ អោយបានលម្អិត ឬ ជ្រើសរើសបច្ចេកវិទ្យាប្លុកឆេនមួយណាមកប្រើប្រាស់ យើងត្រូវសិក្សាឈ្វេងយល់បន្ថែម។ ម៉្យាងវិញទៅ បច្ចេកវិទ្យាប្លុកឆេនសព្វថ្ងៃ មិនមែនគ្រាន់តែប្រើក្នុងការទូទាត់លុយអេឡិចត្រូនិចប៉ុណ្ណោះទេ គឺយើងអាចយកវាទៅប្រើក្នុងផ្នែកផ្សេងៗបានដោយទូលំទូលាយ។

ជាចុងបញ្ចប់ សូមអភ័យទោសរាល់កំហុសឆ្គងនានាដែលបានកើតឡើងដោយអចេតនា ប្រសិនបើមានចំណុចកែលម្អ ឬ សំនួរនានាពាក់ព័ន្ធជាមួយនឹងបច្ចេកវិទ្យាមួយនេះ អាចទំនាក់ទំនងតាមរយៈ អាស័យដ្ឋានអេឡិចត្រូនិច sok.kimheng@gmail.com សូមអរគុណ។