KCHAIN VA BITCOIN TEXNOLOGIYALARIDA TRANZAKSIYA ZANJIRINI STRUKTURALARI

Mahammadjonov Muhammaddiyor Ahmadjon o'g'li
Iqtisodiyot yo'nalishi 1-kurs 25-17 guruh talabasi
Pozilova Gulzodabegim Rustambek qizi
Iqtisodiyot yo'nalishi 1-kurs 25-17 guruh talabasi
Qo'qon Universiteti Andijon filliali
Xalımjanov Abduqunduz Rahimjon o'g'li
"KI va RT" kafedrasi o'qituvchisi
Qo'qon Universiteti Andijon fillialı
https://doi.org/10.5281/zenodo.17977323

Annotatsiya: Ushbu maqolada blokcheyn texnologiyasining kelib chiqisht ishlash mexanizmi, kriptografik asoslari va real sektor uchun taqdim etayotgan ustunliklari yoritilgan shuningdek, blokcheynning tranzaksiyalarni tasdiqlash jarayoni, minerlarning vazifalari hamda xesh funksiyalari orqali ta'minlanadigan xavfsizlik mexanizmlari ko'rib chiqiladi. Maqolada pul o'tkazmalari misolida blokcheynning an'anaviy tizimlardan ustun jihatlari tahlil qilinadi va turli sohalarda qo'llanilishiga doir amalty misollar keltiriladi

Kalit so'zlar: blokcheyn, kriptografiya, xesh kodi, tranzaksiya, miner, taqsimlangan tizim, raqamli imzo, elektron tijorat kriptovalyuta.

Kirish: Raqamli iqtisodiyotning keskin rivojlanishi axborot almashinuvi va tranzaksiyalarni xavfsiz boshqarish masalasını dolzarb qilib qo'ymoqda. So'nggi o'n yillik davomida blokcheyn texnologiyasi eng ishonchli, o'zgartirib bo'lmaydigan va shaffof axborot tizimi sifatida shakllandi Blokcheyn dastlab 1991-yilda raqamlı hujjatlarnt himoya qilish uchun taklif etilgan bo'lsa-da, bugungi kunda moliya. sog'liqni saqlash, elektron tijorat, yer kadastrı, to'lovlar, yetkazib berish tizimlari kabi ko'plab sohalarda keng qo'llanilmoqda. Ushbu texnologiya turli jarayonlarda vositachi tashkilotlarga bo'lgan ehtiyojni kamaytiradi, tranzaksiyalarmı tezlashtiradi va ulardagi firibgarlık ehtimolini butkul bartaraf etadi.

Asosiy qism:

1. Blokcheyn tushunchasi va uning tuzilishi

Blokcheyn (Blockchain) atamasi ikki so'zdan iborat: **block - blok, chain zanjir.** Har bir blok kriptografik shaklda saqlangan ma'lumotlar to'plami bo'lib, barcha bloklar ketma-ket ulangan tarzda yagona zanjimi hosil qiladi. Har bir blok quyidagi ma'lumotlarni o'z ichiga oladi:

1. blokning xesh kodt;
2. undan oldingi blokning xesh kodi;
3. tranzaksiyalar to'plami.

Bloklar o'zaro kriptografik bog'langanligi sababli zanjirning har qanday qismidagi o'zgarish darhol butun tizimda nomuvozanat yuzaga keltiradi. Shu boisdan blokcheynni o'zgartirish, buzish yoki ma'lumotni yashirishning iloji yo'q.

Markazlashmagan tizim va "ochiq daftar" tamoyili

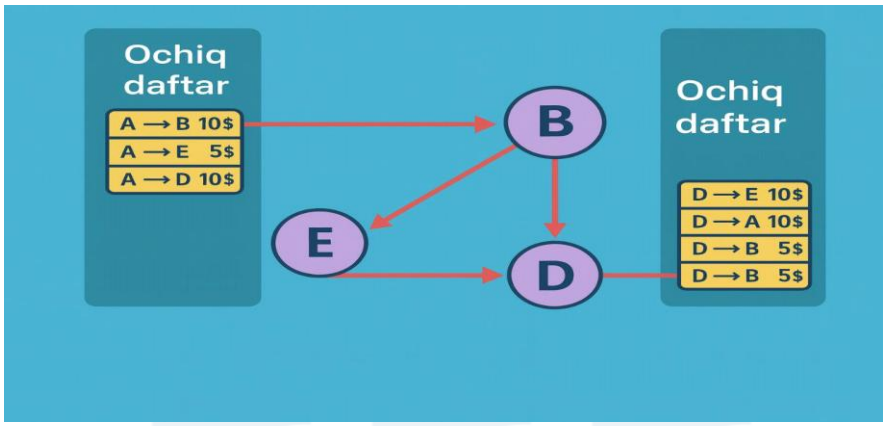
An'anaviy bank va to'lov tizimlarida barcha tranzaksiyalar markaziy server orqali boshqariladi. Blokcheyn esa taqsimlangan tizim (Distributed Ledger Technology - DLT) asosida ishlaydi. Ya'ni, tarmoqning har bir ishtirokchisi daftar nusxasiga ega bo'lishi mumkin.

Misol: A, B, D va E ismli foydalanuvchilar o'zaro pul o'tkazishmoqchi. A da 10$ mavjud bo'lsa, u B ga 55 yuboradi. Bu tranzaksiya "ochiq daftar ga yoziladi va barcha foydalanuvchilar

darhol o'z daftar nusxasini yangilaydi. Keyingi tranzaksiyalar ham xuddi shu tartibda zanjirga qo'shiladi.

Agar A E ga 15$ yubormoqchi bo'lsa, tarmoqdagi barcha ishtirokchilar bunday tranzaksiya imkonsizligini darhol biladi, chunki A da 15$ mavjud emas. Bu tranzaksiya avtomatik tarzda invalid hisoblanadi.

"Ochiq daftar" yordamida tarmoqning barcha ishtirokchilari pul qayerda ekanligini, kimda qancha pul borligini bilishi mumkin. Shu boisdan, ishtirokchilar kim kimga qancha pul o'tkaza olishi yoki olmasligini ham biladi. Masalan, yuqoridagi misolda A E ga 15$ o'tkazmoqchi bo'lsa, tarmoqdagi barcha ishtirokchilar bunday tranzaksiya (AE 15$) bo'lishi mumkin emasligini darhol biladi. Chunki boshida A da 10$ bo'lganligi, 5$ B ga o'tkazilganligi, hozirda esa A da 15$ pul yo'qligini hamma biladi. Shu sababli bu tranzaksiya ochiq daftarga qo'shilmaydi. Bunday tranzaksiyalar invalid (haqiqiy bo'lmagan) tranzaksıya hisoblanadi va uni tarmoqda hech kim tasdiqlamaydi.



1-jadval

Blokcheynda taqsimlangan, ya'ni tarmoqdagi xohlagan shaxs (yoki tugun) daftar nusxası (ledger)ni o'zida saqlashi mumkin bo'lgan **distributed ledger** tizimi ishlatiladi. 1-rasmda keltirgan tarmoqda A, B, D, E tugunlar mavjud. Masalan, zarur bo'lganda ledger A va D tugunlarda yoki tarmoqdagi barcha tugunlarda saqlanishi mumkin. Bu orqali ochiq daftar taqsimlangan holatda saqlanishiga erishiladi va uni markaziy joyda saqlashga ehtiyoj qolmaydi. Daftarning taqsimlangan holatda saqlanishi natijasida daftar nusxasi hamma tugunlarda paydo bo'lishiga olib keladi.

Endi ochiq daftar (tanzaksiyalar zanjiri) nusxasini tarmoqdagi hamma ishtirokchilar orasida sinxronlashtirib, daftar nusxalarining bir-biriga mosligini ta'minlash lozim.

Faraz qilaylik, B E ga 5$ o'tkazmoqchi, ya'nı (B > E 5$). Shunda B E ga 5$ o'tkazmoqchi ekanligini tarmoqqa e'lon qiladi. Tarmoqdagi hamma ishtirokchilar B ning bunday tranzaksiya gilmoqchi ekanligidan xabardor bo'ladi. Bu tranzaksiyaning haqiqiyligini hech kim tekshirib ko'rmaganligi sababli, bu ma'lumot ochiq jurnalga kelib tushmaydi.

Endi bu tranzaksiyani ochiq jurnalga qanday yozilishini bilish uchun miner tushunchasini aniqlashtirib olishimiz kerak.

Miner deb, ochiq daftarni o'zida saqlovchi maxsus tugunga aytiladi. Masalan, 2-rasmda tasvirlangan tarmoqdagi A va D tugunlarni miner deb oladigan bo'lsak, bu minerlarning asosiy vazifasi - bo'lishi kutilayotgan yangi tranzaksiyalar haqiqiyligini tekshirish va uni ochiq daftarga birinchi bo'lib yozishdan iborat. Bu ishlarni birinchi bo'lib bajargan miner "musobaqa"da yutib chiqadi va moliyaviy mukofot - bitcoinga ega bo'ladi.

Minerlar faoliyati va bloklarni tasdiqlash jarayoni

Blokcheynning eng muhim jarayoni - tranzaksiyalarni tasdiqlash. Bunda minerlar (maxsus tugunlar) quyidagi vazifalarni bajaradi:

1) Tranzaksiyaning haqiqiyligini tekshirish

Miner ochiq daftar asosida tranzaksiyaning real yoki soxta ekanligini aniqlaydi. Masalan, B dan E ga yuboriladigan 5$ tranzaksiyada B da zarur mablag' mavjudligini tasdiqlaydi.

2) Maxsus tasodifiy kalitni topish

Blokchenga yangi blok qo'shish uchun minerlar murakkab kriptografik masalani hal qiladi. Topilishi kerak bo'lgan maxsus qiymat odatda 16 lik sanoqsistemasidagi 64 xonali son bo'ladi. Uni birinchi bo'lib topgan miner blokni zanijinga qo'shish huquqiga ega bo'ladi.

3) Mukofot olish

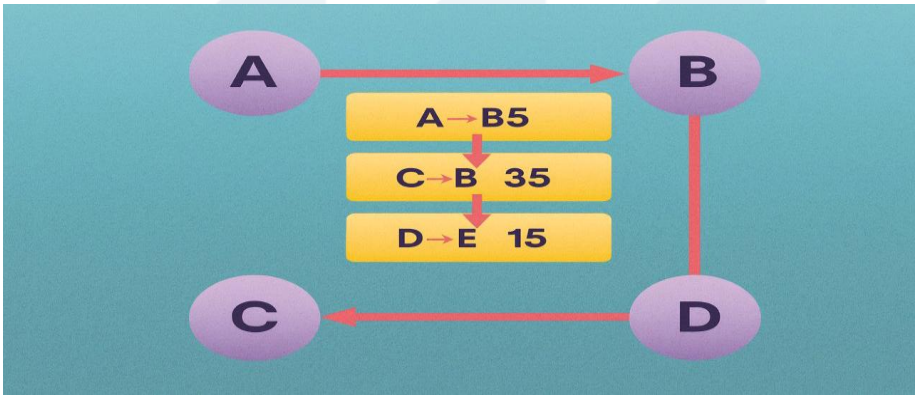
Masalani birinchi bo'lib yechgan miner pul mukofoti -kriptovalyuta (masalan, bitcoin) oladi.

Blokchain yuqoridagi vaziyat uchun quyidagilarni hal qilishda yordarm beradi.

pul o'tkazmasini to'g'ridan to'g'ri (3-tomon ishtirokisiz) amalga oshirish,

pul o'tkazmasını tezroq, o'sha vaqtning o'zida onlayn tarzda bajarish

pul o'tkazmasi uchun olinadigan xizmat haqini kamaytirish.



2-jadval

Endi blokcheyn yuqoridagi holatlar uchun qanday ishlashini ko'rib chiqamiz.

Buxgalteriya sohasida kirim-chiqimlarni qayd etish va kirim-chiqımlar balansini me'yorda ushlab turish uchun **hisob-kitob daftari**dan foydalaniladi.

Blokcheynda harn amalga oshirilgan tranzaksiyalarni qayd etib borish uchun doimiy yangilanib boruvchi "ochiq daftar" qo'llaniladi.

Bizda A (Anvar), B (Botir), D (Davron) va E (Elbek) ismli 4 nafar foydalanuvchidan tashkil topgan blokcheyn tarmog'i mavjud bo'lsin. Bu tarmoqdagi shaxslar 1-jadvalda ko'rsatilgan tartibda bir-birlariga (A B. B D.D E) pul o'tkazishmoqchi.

A da 10$ pul borligi bizga 1-tranzaksıya (A=10$)ni beradi. Endi A B ga 5$ pul o'tkazmoqchi. Shunda, ro'yxatga 2-tranzaksiya (A > B 5$), ya'ni A dan B ga 5$ pul o'tkazildi, degan ma'lumot tushadi. Bu valid (haqiqiy) tranzaksiya hisoblanadi. Hosil bo'lgan 2-tranzaksiya 1-tranzaksiyaga qo'shib qo'yiladi va ular orasida zanjir hosil bo'ladi. Undan keyin B D ga 3$ pul o'tkazmoqchiligi haqidagi ma'lumot (B > D3$) "Ochiq daftar ga yozib qo'yiladi. Ushbu 3-tranzaksiya ham mavjud tranzaksiyalar

Xesh funksiyalari orqali xavfsizlikni ta'minlash

Har bir blokdagi xesh kod quyidagi sabablarga ko'ra juda muhim: Blokdagi eng kichik o'zgarish xeshni to'liq o'zgartiradi. Agar tajovuzkor 2-blokni o'zgartirsa, 3-blokdagi "oldingi

xesh" qiymati mos kelmaydi va zanjir buziladi, Natijada, tizim bunday o'zgarishlarni darhol aniqlaydi va bekor qiladi.Shu sababli blokcheyn juda yuqori xavfsizlikka ega..

Blokcheynning qo'llanilish sohalari

Raqamli identifikatsiya: Civic, UniqulD kabi tizimlar biometrik identifikatsiyani blokcheyn asosida uyg'unlashtiradi.

Mualliflik huquqi: Stampery, Ascribe platformalari raqamli asarlarni himoya qilishda blokcheyndan foydalanadi.

Xulosa

Blokcheyn texnologiyasi o'zining xavfsizlik, shaffoflik, tezkorlik va vositachilarsiz ishlash xususiyatlari bilan zamonaviy raqamli tizimlarning asosiy tayanchiga aylanmoqda. Taqsimlangan daftar tamoyili, xesh funksiyalari, tranzaksiyalarni tasdiqlovchi minerlar faoliyati blokcheynning buzilmas strukturasi va ishonchliligini ta'minlaydi. Bugungi kunda blokcheyn nafaqat kriptovalyuta, balki sog'liqni saqlash, elektron tijorat, kadastr, bank va boshqa ko'plab sohalarda samarali qo'llanilmoqda. Ushbu texnologiya kelajakda raqamli iqtisodiyotning barcha jabhalarida yetakchi o'rin egallashi shubhasiz.

Adabiyotlar, References, Литературы:

1. Nakamoto S. Bitcoin: Tengdoshlarning elektron pul tizimi, 2008 yil.
2. Mougayar W. Biznes blokcheyn. Wiley, 2016 yil.
3. Crosby M., Pattanayak P. Blockchain Technology: Beyond Bitcoin, 2016.
4. Swan M. Blockchain: Yangi Iqtisodiyot uchun loyiha. O'Reilly Media, 2015 yil.
5. Antonopoulos A. Bitcoinni o'zlashtirish, 2017 yil.
6. Uzbekcoding, "BlockChain asoslari bo'yicha qo'llanma", 2022.