# 67-dars. BLOCKCHAIN TEXNOLOGIYASI

Satoshi Nakamoto,
bitcoin asoschisi

**TAYANCH TUSHUNCHALAR**

**Blokchain** – muayyan qoidalarga muvofiq tuzilgan va axborotni o'z ichiga olgan bloklar uzluksiz ketma-ket zanjiri. Blok zanjirlarining nusxalari mustaqil ravishda turli kompyuterlarda saqlanadi.

**Bitcoin (bitkoin)** atamasi inglizcha *bit* – ikkilik sanoq tizimidagi informatsiya birligi va *coin* – tanga so'zlarining qisqartmasidan iborat.

**Tranzaksiya** (ingl. *transaction*) – blockcheynda ma'lumotlarni saqlash operatsiyasi.

Blokcheyn texnologiyasi butun dunyoda ommalashib bormoqda. Blokcheyn oxirgi o'n yillikda paydo bo'lgan texnologiyalardan biridir. Bu texnologiya bugungi kunda eng xavfsiz, qulay va ishonchli texnologiya hisoblanadi. Blokcheyn atamasi birinchi marta 1991-yilda tadqiqotchilar guruhi tomonidan tasvirlangan va dastlab raqamli hujjatlarni belgilash uchun mo'ljallangan ma'lumotni o'z ichiga olgan.

Hozirda sog'liqni saqlash tizimi, FXDY, turizm, elektron tijorat va moliya, bank to'lov tizimlari, soliq tizimi, yer resurslarini ro'yxatga oluvchi kadastr tizimi kabi bir qancha sohalarda blokcheyn texnologiyasidan foydalanib kelinmoqda. Shaffoflik ta'minlanishi muhim bo'lgan sohalarda blokchain texnologiyasidan foydalanish yuqori samara beradi.

Blockcheyn atamasi ikkita elementdan iborat: inglizcha ***block*** – blok va ***chain*** – zanjir.

Blok kriptografik shaklda taqdim etilgan ma'lumotlar bo'lsa, blokchain ketma-ket ulangan zanjir ko'rinishidagi bloklar ro'yxati yoki bloklarga taqsimlangan ma'lumotlar bazasi hisoblanadi. Bloklar zanjiri kriptografiya, raqamli imzo va xesh funksiyalar yordamida shakllantirilgan strukturaga ega. Zanjirning har bir bloki o'zida undan avvalgi blok haqidagi ma'lumotni saqlaydi. Tranzaksiya natijasida zanjirdagi bloklar ko'payib boradi, ya'ni mavjud bloklar zanjiriga yangi blok qo'shilib boradi. Blokchain texnologiyasi asosida saqlanadigan ma'lumotlar xavfsiz va shaffof bo'lib, ushbu ma'lumotlar bazasidan blokni o'chirish yoki almashtirish mumkin emas.

Demak, blokcheyn bilan batafsilroq tanishamiz.

Tasavvur qiling, Hamid va Umar – boshqa-boshqa davlatlarda yashaydigan biznes hamkorlar. Hamid Umarga 2000$ miqdoridagi pulni jo'natishi lozim. Pul o'tkazmasini amalga oshirish uchun "Western Union", "Contact", "Unistream", "Moneygram" kabi tizimlar yoki biror bank kabi 3-ishonchli tomon kerak. Hamid o'zi yashab turgan shahardagi 3-tomon bo'linmasiga

borib, pulni qayerga va kimga o'tkazilishi kerakligini aytadi va pulni beradi. Hamid bu haqda Umarga ham xabar beradi. Umar ham o'zi yashab turgan shahardagi 3-tomon bo'linmasiga boradi va shaxsini tasdiqlovchi hujjatlari yordamida pulni oladi. Ishonchli tomon bu pulni o'tkazib berganligi uchun o'z xizmat haqi (masalan, 5$)ni oladi. Ushbu pul o'tkazmasi bajarilishi 3-tomonga bog'liq va uning uchun ma'lum vaqt kerak bo'ladi. Agar pul o'tkazish bank orqali amalga oshirilsa, taxminan 3–4 kun, pul o'tkazish tizim (masalan, Western Union)lari orqali o'tkazilsa, ancha tez amalga oshiriladi. Pul o'tkazish ba'zi davlatlarda 15–20 daqiqada, ayrimlarida esa 24–72 soatda amalga oshirilishi mumkin.

**TAYANCH TUSHUNCHALAR**

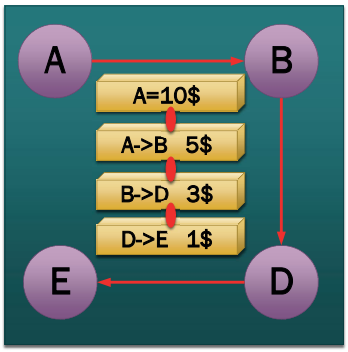
**Minerlar – blockchain tizimining maxsus ishtirokchilari. Ularning kompyuterlari boshqa ishtirokchilar tranzaksiyalarini tekshirish uchun moslashgan bo'ladi.**

Blokchain yuqoridagi vaziyat uchun quyidagilarni hal qilishda yordam beradi:

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

–pul o'tkazmasini tezroq, o'sha vaqtning o'zida onlayn tarzda bajarish;

–pul o'tkazmasi uchun olinadigan xizmat haqini kamaytirish.

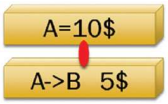



Endi blokcheyn yuqoridagi holatlar uchun qanday ishlashi ko'rib chiqamiz.

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

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

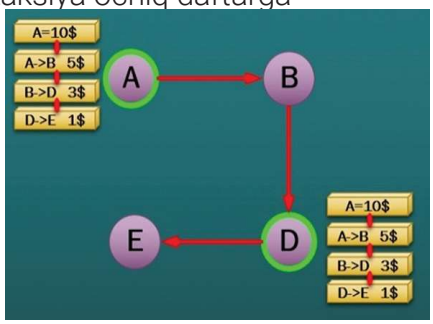
Bizda A (Anvar), B (Botir), D (Davron) va E (Elbek) ismli 4 nafar foydalanuvchidan tashkil topgan blokcheyn tarmog'i mavjud bo'lsin. Bu tarmoqdagi shaxslar 1-jadvalda ko'rsatilgan tartibda bir-birlariga (A B, B D, D E) pul o'tkazishmoqchi.




A da 10$ pul borligi bizga 1-tranzaksiya (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 > D 3$) "Ochiq daftar"ga yozib qo'yiladi. Ushbu 3-tranzaksiya ham mavjud tranzaksiyalar

zanjiri oxiriga yangi tranzaksiya sifatida bog'lab qo'yiladi. Xuddi shu tarzda D E ga 1$ pul o'tkazmoqchiligi haqidagi ma'lumot (D > E 1$) ham ro'yxatga, ya'ni "Ochiq daftar"ga yoziladi va u ham tranzaksiyalar zanjiriga yangi tranzaksiya sifatida biriktirib qo'yiladi. Shu tarzda hosil qilingan ro'yxatga "Ochiq daftar", ya'ni ***tranzaksiyalar zanjiri*** deyiladi.

"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) tranzaksiya hisoblanadi va uni tarmoqda hech kim tasdiqlamaydi.




Blokcheynda taqsimlangan, ya'ni tarmoqdagi xohlagan shaxs (yoki tugun) daftar nusxasi (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 (tarnzaksiyalar zanjiri) nusxasini tarmoqdagi hamma ishtirokchilar orasida sinxronlashtirib, daftar nusxalarining bir-biriga mosligini ta'minlash lozim.

Faraz qilaylik, B E ga 5$ o'tkazmoqchi, ya'ni (B > E 5$). Shunda B E ga 5$ o'tkazmoqchi ekanligini tarmoqqa e'lon qiladi. Tarmoqdagi hamma ishtirokchilar B ning bunday tranzaksiya qilmoqchi 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.

Miner musobaqada g'olib chiqish uchun quyidagilar bajarilishi lozim:

– yangi, tekshirilmagan tranzaksiyani olib, uning haqiqiyligini tekshirish kerak. Daftarning ochiqligi va kimda qancha pul borligi haqidagi ma'lumotlar tranzaksiyaning haqiqiyligini aniqlashga yordam beradi. Masalan, miner ochiq daftar orqali B da E ga o'tkazishi uchun yetarlicha mablag' (5$) borligini osongina hisoblay oladi va bu o'tkazmani amalga oshirish mumkinligini tasdiqlaydi;

– miner maxsus tasodifiy kalitni tez izlab topishi kerak. Shunda u topilgan kalit yordamida yangi tranzaksiyani ochiq daftardagi tarnzaksiyalar zanjiriga tezroq qo'shish imkoniyatiga ega bo'ladi. Kalit, odatda, 16 lik sanoq sistemasidagi 64 xonali sondan iborat bo'ladi. Kalitni birinchi bo'lib topgan minerga moliyaviy mukofot bitkoin beriladi.

Masalan, D tugundagi miner yuqoridagi ikkita ishni bajarib bo'ldi, deylik. Bu holatda D tugun (B > E 5$) tarnzaksiya haqiqiy tranzaksiya ekanligini tarmoqqa e'lon qiladi. Tarmoqdagi boshqa minerlar bu xabarni olishlari bilan, uni o'zlaridagi tranzaksiyalar zanjiriga yangi blok sifatida qo'shib qo'yishadi. Shu tarzda minerlar o'z ishlarini davom ettiradi. Hozirgi holatda D miner musobaqada yutib chiqqan bo'lsa, kelasi safar A miner yutib chiqishi mumkin.

Blok ichida saqlanadigan ma'lumotlar blokcheyn turiga bog'liq.


## Genesis loki

Masalan, bitkoinlar blokida jo'natuvchi va qabul qiluvchi shaxs hamda o'tkaziladigan bitkoin miqdori haqidagi ma'lumotlar mavjud.


Bitkoin blokiga misol:

zanjirdagi 1-blok *Genesis bloki* deb ataladi. Zanjirdagi har bir yangi blok oldingi blok bilan bog'langan bo'ladi.


Blokda ham xesh mavjud. Xeshni "har bir blok uchun yagona bo'lgan barmoq izi", deb tushunish mumkin. U blok va uning tarkibini aniqlaydi hamda barmoq izi kabi yagona bo'ladi. Shuning uchun, blok yaratilganidan so'ng, blok ichidagi har qanday o'zgarish xeshni o'zgartirishga olib keladi.

Blokcheynning har bir bloki o'zida 3 xil ma'lumotni saqlaydi:

1) blokning xesh kodi;

2) undan oldingi blokning xesh kodi;

3) tranzaksiyalar.


Quyidagi misolda 3 blokli zanjir borligini ko'rishimiz mumkin. 1-blokdan oldin hech qanday blok yo'q. Shuning uchun u oldingi blokni o'z ichiga olmaydi. 2-blokda esa 1-blok xeshi bor va u 2AF5 ga teng. 3-blokda esa 2-blokning xeshi bor va u 6D3N ga teng.

Shunday qilib, barcha bloklar oldingi bloklarning xeshlarini o'z ichiga oladi. Bu blokcheyn xavfsizligini ta'minlovchi texnika hisoblanadi. Kelinglar, u qanday ishlashini ko'rib chiqaylik.

Masalan, tajovuzkor 2-blok ma'lumotlarini o'zgartirganligi uchun 2-blok xeshi ham o'zgaradi. 3-blokda hali ham 2-blokning eski xeshi saqlanib qolaveradi. 2-blokning to'g'ri xeshiga ega bo'lmagan 3-blok va undan keyingi barcha bloklar bekor qilinadi.


Shuning uchun ham bitta blokning o'zgarishi keyingi barcha bloklarning tez bekor qilinishiga sabab bo'ladi.

Rivojlanishning dastlabki bosqichida blokcheyn texnologiyasi faqat kriptovalyuta uchun platforma sifatida ishlatilgan. Keyin moliyaviy institutlar bu texnologiyadan foydalana boshladi. Hozirgi vaqtda blokcheyn turli tizimlarda qo'llanilmoqda. Masalan, Stampery elektron notariusi blokcheyn yordamida turli bitim (kelishuv)lar tasdiqlab berilmoqda. Bundan tashqari, blockchain mualliflik huquqi va shaxsiy ma'lumotlarni tartibga soluvchi qonunlar doirasida ham qo'llaniladi. Ascribe xizmati blockcheyn yordamida rassom va ijodkor shaxslarga o'z mualliflikini tasdiqlashda qo'l kelmoqda. Civic (CVC) va UniquID Wallet ilovalari biometrik himoyadan foydalanadigan odamlarga soxtalashtirish mumkin bo'lmagan raqamli identifikatorlarni yaratish imkonini beradi (faqat vaqt o'tishi bilan shaxsiy guvohnomalarni almashtirish mumkin).

## AMALIY FAOLIYAT

| № | Topshiriqlar |
|---|---|
| **1-topshiriq. Test savollariga javob bering.** | |
| 1 | **Blokcheyn – … .**<br>a) tranzaksiyalar bilan ishlaydigan dastur;<br>b) muayyan qoidalarga muvofiq tuzilgan va axborotni o'z ichiga olgan bloklar uzluksiz ketma-ket zanjiri;<br>c) buzg'unchining biror maqsad yo'lidagi harakati;<br>d) ma'lumotlarni saqlash operatsiyasi. |
| 2 | **Bitkoinning asoschisi kim?**<br>a) Bill Gates;<br>b) Satoshi Nakomoto;<br>d) Steve Jobs;<br>e) Blez Paskal. |
| 3 | **Blockcheyn texnologiyasining ishlash prinsipini tushuntiring.** |

### SAVOL VA TOPSHIRIQLAR

1. Blockchain nima?
2. Blockchainning maqsadini tushuntiring.
3. Ochiq daftar nima uchun kerak?
4. Blockchain texnologiyasining afzalliklari va kamchiliklari nimada?

### UYGA VAZIFA

1. Blockchainning turlarini o'rganing.
2. "Blockchain qanday ishlaydi?" mavzusida taqdimot tayyorlang.
3. Blockchain mavzusiga oid boshqotirma tuzing.