O‘ZBEKISTON RESPUBLIKASI
OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

MIRZO ULUG‘BEK NOMIDAGI
O‘ZBEKISTON MILLIY UNIVERSITETI

R.H. ALAYEV

BLOKCHEYN TEXNOLOGIYALARI

O‘ZBEKISTON RESPUBLIKASI
OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

MIRZO ULUG‘BEK NOMIDAGI
O‘ZBEKISTON MILLIY UNIVERSITETI

R.H. ALAYEV

BLOKCHEYN TEXNOLOGIYALARI

O‘quv qo‘llanma

O‘zbekiston Milliy Universiteti Kengashi tomonidan
o‘quv qo‘llanma sifatida tavsiya etilgan.

Toshkent-2024

UO'K: 004.65(075.8)

KBK: 32.973-018.2ya73

A45

Alayev R.H.

Blokcheyn texnologiyalari, O'quv qo'llanma / Alayev R.H. O'zbekiston Milliy Universiteti Kengashi tomonidan o'quv qo'llanma sifatida tavsiya etilgan. "Farg'ona: "Farg'ona Tipograf Xizmat" nashriyoti, 2024. – 128 b.

Taqrizchilar: **Jo'rayev G. U.** *O'zMU "Axborot xavfsizligi" kafedrasi professori, fizika-matematika fanlari doktori*

K.F. Kerimov *Al-Xorazimiy nomidagi TATU «Tizimli va amaliy dasturlashtirish» kafedrasi mudiri, texnika fanlari doktori*

Mazkur o'quv qo'llanma 60610300 – Axborot xavfsizligi (sohalar bo'yicha) ta'lim yo'nalishining talabari uchun mo'ljallangan. O'quv qo'llanmada blokcheyn asoslari, kriptovalyutalar, elliptik egri chiziqlar kriptografiyasi, bitkoin kriptovalyutasi protokollari, mayning algoritmi, bitkoin tarmog'i, efirium kriptovalyutasi va uning ishlash prinsipi masalalari yoritilgan.

ISBN 978-9910-9486-1-9

KIRISH

Jahonda blokcheyn texnologiyalari keng miqyosda iqtisodiyot, moliya, bank, tibbiyot, farmasevtika, sug'urta, kadastr, transport, logistika va boshqa sohalarda jadal suratda joriy qilinmoqda. Bu esa ushbu sohalarda qalbaki mahsulotlarni aniqlash va bartaraf etish, xizmat ko'rsatish jarayonini tezlashtirish, ortiqcha aralashuvlarni oldini olish, xarajatlarni kamaytirish, ma'lumotlarning xavfsizligini, butunligini, foydalanuvchanligini, mualliflik huquqini, ruxsatsiz foydalanishning oldini olishni ta'minlash va boshqa imkoniyatlarni taqdim etmoqda.

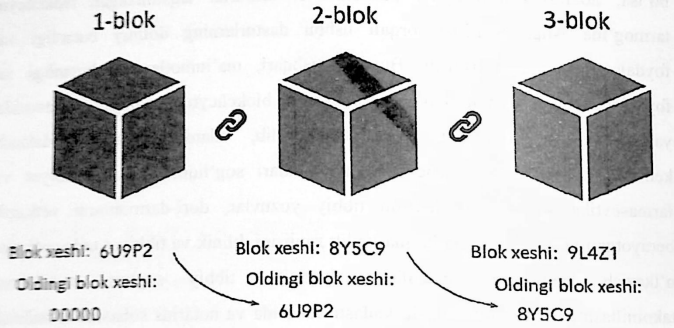
Dastlabki yaratilgan kriptovalyutalar asosan elektron to'lovlarni hech qanday markazlashgan boshqaruvchi organsiz amalga oshirish imkonini bergan bo'lsa, hozirgi kriptovalyuta platformalari dasturlar taqsimlangan blokcheyn tarmog'ida ishga tushirish orqali ushbu dasturlarning doimiy butunligi va foydalanuvchanligini oshirdi. Bundan tashqari, ma'lumotlarning butunligi va foydalanuvchanligi muhim bo'lgan sohalarda blokcheyn texnologiyalari asosida yangi axborot tizimlari yaratilgan bo'lib, ulardan keng foydalanib kelinmoqda.Masalan, blokcheyn texnologiyalari sog'liqni saqlash, tibbiyot va farmasevtika sohasidagi elektron tibbiy yozuvlar, dori-darmonlarni yetkazib berayotgan vositachilarning ketma-ketlik zanjirini, klinik va tibbiyot tadqiqotlarini o'tkazish, bemorlarni masofadan kuzatish, tibbiy sug'urta tartiblarini takomillashtirish va tahlil qilish, kadastr sohasida va notarius sohasida bitimlarda va egalik huquqini ta'minlash maqsadida qo'llanila boshlangan.

Mazkur o'quv qo'llanma talabalar va ushbu sohaga qiziquvchi yoshlarning "Blokcheyn texnologiyalari" bo'yicha bilim va ko'nikmalarini shakllantirishga xizmat qiladi.

I BOB. BLOKCHEYN ASOSLARI

1.1. Blokcheyn tushunchasi

Blokcheyn (ingliz tilida – "blockchain") – bu kriptografik usulda bog'langan ma'lumotlar bloklari ro'yxati. Har bir blokda o'zidan oldingi blokning kriptografik xesh qiymati, hamda vaqt qiymati va tranzaksiyalar to'g'risidagi ma'lumotlar mavjud (1-rasm). Blokcheynda ma'lumotlar hajmi kundan kunga ko'payib bormoqda. Buni ayniqsa, dunyoda juda mashhur Bitkoin kriptovalyutasi misolida ko'rish mumkin. Ko'pgina hukumatlar va yetakchi banklar blokcheyn kontsepsiyasiga asoslanib, o'zlarining odatiy operatsiyalarini amalga oshirishni boshladilar. Ushbu platformaning dasturlari va potentsiali juda katta, blokcheyn turli sohalarda bitimlarni amalga oshirish usulini o'zgartiradi deb ishoniladi.



1-rasm. **Blokcheyndagi bloklar**

1.2. Kriptovalyuta tushunchasi

Kriptovalyuta – bu to'liq avtomatik rejimda ishlaydigan, markazlashtirilmagan to'lov tizimi (kriptovalyutani boshqaradigan ichki yoki tashqi boshqaruvchi yoki shunga o'xshash organlar yo'q) tomonidan ichki to'lov birliklari hisobini yuritadigan raqamli valyutaning (virtual pul) bir turi. O'z-o'zidan, kriptovalyuta hech qanday maxsus material yoki elektron shaklga ega

emas – bu shunchaki raqamlar ketma-ketligi bo‘lib, u to‘lov birliklari sonini anglatadi. U ma’lumotlar uzatish protokolining axborot paketida yoziladi, odatda xuddi tranzaksiya haqidagi boshqa ma’lumotlar kabi shifrlanmaydi. Shu bilan birga, manzil (kriptovalyutada foydalanuvchi hisob raqami, hamyon adresi) ni yaratish va u bilan operatsiyalarni amalga oshirishda avtorizatsiyani amalga oshirish kriptografik usullarga asoslangan: (ochiq kalitli kriptografiyaga asoslangan elektron raqamli imzo, biron bir tranzaksiya orqali kelgan mablag‘ni sarflash faqat ushbu tranzaksiyada ko‘rsatilgan manzilga mos keladigan yopiq kalit egasiga beriladi).

“Kriptovalyuta” atamasi 2011-yilda Forbes jurnalida chop etilgan Bitkoin tizimi to‘g‘risidagi maqoladan keyin keng qo‘llanila boshlandi. Bitkoin yaratuvchisi va boshqa ko‘plab mualliflar “elektron pul” (electronic cash) atamasidan foydalangan.

Boshqa elektron to‘lov tizimlaridan farqli ravishda kriptovalyutalar real pullarning ishtirokisiz paydo bo‘ladi.

Har qanday kriptovalyuta to‘lov vositasi statusiga ega emas (lekin ba’zi davlatlar bitkoinni tan olgan. Masalan, Yaponiya). Virtual pul quyidagi sabablarga ko‘ra ommalashdi:

Keng tarqalganligi, universallik. Hamyonni har qanday kompyuterda, smartfonda yoki planshetda turli xil operatsion tizimlarda yaratishning osonligi.

To‘lov operatsiyalarining soddaligi, ochiqligi. Kiruvchi va chiquvchi operasiyalarning (tranzaksiyalarning) to‘liq tarixining vaqt cheklovisiz saqlanishi.

Kriptovalyutani ishlab chiqarish tizimining har bir uzeli teng huquqli. Hamyonni blokirovka qilish, to‘lovlarni bekor qilish va nazorat qilish huquqiga ega yagona markazning yo‘qligi.

Maksimal anonimlik to‘lov tizimining mustaqilligini oshiradi. To‘lovlarni amalga oshirayotganda hamyon manzilni ko‘rsatiladi xolos. Ya’ni hamma mablag‘ qaysidir hamyondan boshqa bir hamyonga o‘tganini ko‘rishi mumkin. Lekin ushbu hamyonlarning aslida egasi kimligini (shaxsini) blokcheyndan aniqlay olmaydi.

1.3. Blokcheyn avlodlari

Blokcheyn texnologiyasining jadal rivojlanishi va taraqqiyoti tufayli uni qo'llashning ko'plab turlari paydo bo'ldi. Bu yerda tavsiflanadigan 3 ta avlod dastlab Melani Suon (Melanie Swan) ning O'Reilly Media tomonidan 2015-yilda nashr etilgan "Blockchain: Blueprint for a New Economy" kitobida tasvirlangan bo'lib, u yerda turli xil yechimlar ushbu darajalarga ajratilgan.

Deyarli barcha blokcheyn platformalari, biroz istisnolar bilan, bir xil funksiyalarni va joriy etish imkoniyatlarini taqdim etadi.

Tobora ko'proq yangi paydo bo'layotgan blokcheyn platformalari aqlli shartnomalarni ishlab chiqishni, hamda barcha blokcheyn avlodlariga tegishli funksiyalarni qo'llab-quvvatlaydi.

Blokcheyn texnologiyalarini mantiqiy klassifikasiyalash orqali avlodlarga ajratish, ularning hozirgi ishlatilishi, evolyutsiyasi va kutilayotgan evolyutsiyasiga asoslanadi. Hozirda blokcheyn texnologiyasinning quyidagi avlodlari mavjud:

Blokcheyn 1.0: Valyuta. Ushbu avlod bitkoin kriptovalyutasi yaratilishi bilan 2009-yilda paydo bo'ldi. Ushbu avloddagi blokcheynlar asosan to'lovlarni amalga oshirishda qo'llanilgan.

Blokcheyn 2.0: **Smart shartnomalar.** Blokcheynning ikkinchi avlodi moliyaviy xizmatlar va aqlli shartnomalar sohasida joriy etildi. Bu yerda valyutalar, moliya va birjalar bilan cheklanib qolmagan dasturlar mavjud. Ethereum, Hyperledger va boshqa nisbatan yangi blokcheyn platformalari blokcheyn 2.0 sifatida baholandi. Ushbu avlod haqidagi dastlabki qarashlar blokcheynni boshqa maqsadlarga yo'naltirish to'g'risidagi g'oyalar bilan boshlandi, bunday g'oyalar 2010-yilda paydo bo'lgan.

Blokcheyn 3.0: **DApps**. Blokcheynning uchinchi avlodi moliya sanoatidan tashqarida bo'lgan dasturlarni amalga oshirish bilan bog'liq, masalan, hukumat, sog'liqni saqlash, ommaviy axborot vositalari, san'at va huquq sohasida qo'llaniladi. Shunga qaramay, blokcheyn 2.0 singari, ushbu avlodga Ethereum, Hyperledger va aqlli shartnomalar dasturlashtirilishi mumkin bo'lgan yangi

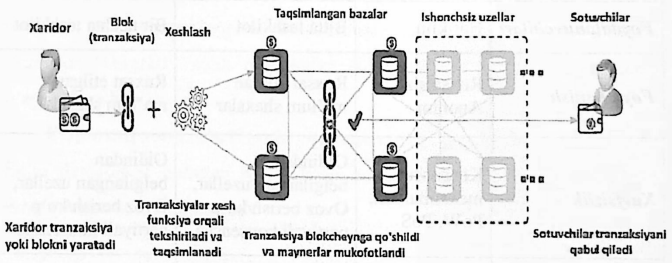
blokcheynlar kiradi. Ushbu avlod blokcheyni 2012-yilga kelib paydo bo'lgan. ***DApps*** – bu taqsimlanagan dasturining qisqartmasi. U markazlashmagan uzellar tarmog'ida ishlaydi.

1.4. Blokcheyn turlari

Blokcheynning quyidagi turlari mavjud:

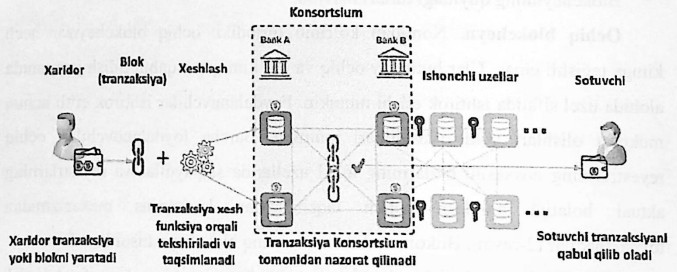
Ochiq blokcheyn. Nomidan ko'rinib turibdiki, ochiq blokcheynlar hech kimga tegishli emas. Ular butunlay ochiq va har kim qaror qabul qilish jarayonida alohida uzel sifatida ishtirok etishi mumkin. Foydalanuvchilar ishtirok etish uchun mukofot olishlari yoki olmasliklari mumkin. Barcha foydalanuvchilari ochiq reyestrlarning nusxasini o'zlarining lokal uzellarida saqlaydilar va reyestrlarning aktual holatini aniqlash uchun taqsimlangan konsensus mexanizmidan foydalanadilar (2-rasm). Bitkoin va Ethereum ochiq blokcheyn hisoblanadi.

Yopiq blokcheynlar. Yopiq blokcheynlar hamma uchun ham foydalanish imkoni mavjud emas. Ya'ni, ular faqat reyestrdan umumiy foydalanish uchun qaror qilgan konsortsium yoki shaxslar guruhi uchun ochiqdir (3-rasm). Hozirda ushbu toifadagi *HydraChain* va *Quorum* kabi blokcheynlar mavjud. Prinsipial jihatdan, agar kerak bo'lsa, ushbu ikkala blokcheyn ochiq rejimda ishlashi ham mumkin, ammo ularning asosiy maqsadi yopiq foydalanishdir.



2-rasm. **Ochiq blokcheyn**

Konsortsium. Blokcheynning ushbu turida faqat bir guruh tashkilotlar tranzaksiyalarni tekshirishi va qo‘shishi mumkin. Bu yerda blokcheyn ochiq bo‘lishi yoki faqat ma’lum guruhlarga ruxsat berilishi mumkin. Blokcheyn konsorsiumi kross-tashkilotlar uchun ishlatiladi. U faqat oldindan aniqlangan uzellar tomonidan boshqariladi.



3-rasm. **Konsortsium blokcheyn**

1-jadvalda blokcheyn turlarining qiyosiy tahlili keltirib o‘tilgan.

1-jadval. Blokcheyn turlarining qiyosiy tahlili

	Ochiq	**Yopiq**	**Konsorsium**
Foydalanuvchilari	Har kim	Bitta tashkilot	Bir nechta tashkilot
Foydalanish	Ruxsatsiz, Anonim	Ruxsat etilgan ma’lum shaxslar	Ruxsat etilgan ma’lum shaxslar
Xavfsizlik	Konsensus mexanizmlari, PoW, PoS	Oldindan belgilangan uzellar, Ovoz berish/ko‘p partiyali konsensus	Oldindan belgilangan uzellar, Ovoz berish/ko‘p partiyali konsensus
Tranzaksiyalarni tasdiqlash tezligi	Sekin	Oson va tez	Oson va tez

1.5. Kriptovalyutalarning kamchiliklari

Kalitlarning xavfsizligini ta'minlash muammosi. Kalitni yo'qotish xavfi ham mavjud, hamyonga egalik huquqini ta'minlovchi kalit yo'qotilsa, ushbu hamyondagi mablag'ni na hamyon egasi va na boshqa kishi ishlata oladi. Agar kalit o'g'irlansa, unda hamyondagi barcha mablag'ga boshqalar (o'g'irlagan shaxslar) egalik qiladi, hamda bu jarayonni orqaga qaytarishning deyarli imkoni yo'q. Chunki yuqorida aytilganidek, bu kriptovalyutani nazorat qiladigan bironta organ (bank) mavjud emas. Ba'zi bir servislar mavjud bo'lib, ular yordamida foydalanuvchi kriptovalyuta hamyonini ochib, foydalanishi mumkin. Bunda foydalanuvchi telefon raqami, elektron pochtasini ko'rsatib ro'yxatdan o'tadi. Bu esa anonimlikni buzadi. Ya'ni kriptovalyutalardan fodalanish maqsadlaridan biri bu anonimlik. Lekin ushbu servislarning afzaligi – bu hamyonga kirish parolini unutganda elektron pochta yoki telefon raqami orqali uni qayta tiklash imkonini beradi. Lekin buning yomon tomoni, hamyonga egalik huquqini tasdiqlovchi kalitdan ushbu servis yaratuvchilari ham foydalanishi mumkin. Bu degani ular to'liq foydalanuvchining hamyonini boshqaradi. Agar ularning tizimini (servisini) buzib kirishsa, unda barcha mijozlarning kalitlari o'g'irlab olinishi mumkin. Bunday holat tarixda sodir bo'lgan.[1]

Kursning tez o'zgarib turishi. Kriptovalyuta kursining o'zgarishi natijasida siz yo'qotishlarga duch kelishingiz, ham foyda olishingiz mumkin. Hammasi "tangalar" sotib olingandan so'ng valyuta kursining qay tarzda o'zgarishiga bog'liq.

Kriptovalyutani cheklovchi qonunlarning paydo bo'lishi ehtimoli. Ba'zi davlatlarda nisbatan tan olingan bo'lsa ham ko'p mamlakatlarda bu turdagi valyutalar cheklangan.

[1] https://www.gazeta.ru/tech/2021/08/11/13855244/poly.shtml

1.6. Kriptovalyutalarning afzalliklari

Raqamli pullarning ko‘pgina afzalliklari Bitkoin misoli sifatida o‘rganiladi. Shuning uchun, oddiy so‘zlar bilan kriptovalyuta nima degan savolni o‘rganganda, BTC nazarda tutadi. BTC – bitkoin birligi simvoli.

Bitimlarning to‘liq shaffofligi. O‘tkazmani (tranzaksiyani) faqat hamyon egasi amalga oshirishi mumkin va u tranzaksiyani amalga oshirishi bilanoq, hech kim operatsiyani bekor qila olmaydi.

Anonimlik darajasining yuqoriligi. Tizim foydalanuvchilari uchun faqat hamyon manzili mavjud, shaxsiy ma’lumotlar nashr etilmaydi va uzatilmaydi.

Kafolatlangan valyuta defitsiti. Ishlab chiqarilgan tangalar sonida qat’iy cheklov mavjud, bu Bitkoinning hisoblash algoritmida ko‘rsatilgan. Lekin hozir ba’zi boshqa turdagi kriptovalyutalar ham mavjud bo‘lib, ularda istalgancha yangi kriptovalyutani ishlab chiqish mumkin. Masalan: *PPCoin, Novacoin, Sifcoin*

Inflyatsiyaning yo‘qligi. Kriptovalyutaning raqamli xususiyati uning haqiqiy valyutalar kurslariga bevosita ta’sir ko‘rsatadigan iqtisodiy, siyosiy, tabiiy omillardan mustaqilligini ta’minlashga imkon beradi. Ya’ni u hech qanday davlat iqtisodiyoti, mavqeyi, boyligi va boshqa holatlarga bog‘lanmagan. Uning kursi asosan bozordagi talab va taklif asosida o‘zgaradi.

1.7. Kriptovalyutani olish usullari

Kriptovalyutani quyidagi usullar bilan olish mumkin:

O‘zingizning kompyuteringizda mayning qilish. Bu usul hozir samarasiz. Lekin oldin shu usul bilan ancha kriptovalyuta ishlab topilgan.

Mayning pullariga qo‘shilib mayning qilish. Bu usul hozir keng tarqalgan. Bu usulda bir necha kishi o‘zlarining mayning qurilmalari quvvatini birlashtirib, birgalikda mayning qiladilar.

Joriy kurs bo‘yicha sotib olish. Ma’lum birjalar yoki onlayn valyuta almashtirish servislari orqali sotib olish mumkin.

Kriptovalyutalarning investitsiyalar sohasida qo'llanilishi ham ommalashib bormoqda.

Kriptovalyuta tangalarini yaratishda ishlatiladigan blokcheyn texnologiyasi raqamli pullarning cheksiz sonli turlarini yaratishga imkon beradi. Ammo hamma kriptovalyutalar ham yuqori mashhurlikka erisha olmaydi va ko'p sonli foydalanuvchilarni mayningga (yangi kriptovalyuta ishlab chiqarish jarayoni) jalb eta olmaydi. Rivojlangan tarmoqsiz (ya'ni keng tarqalmagan) "tangalar (kriptovalyuta birligi)" soni minimal bo'ladi va bunday "valyuta" jamoatchilikni qiziqtirmaydi.

Keng tarqalgan kriptovalyutalar:

Bitkoin. Kripto valyutaning birinchi varianti 2009-yilda paydo bo'lgan.

Efirium. 2015-yilda yaratilgan. Ushbu texnologiya bitimlarni ro'yxatdan o'tkazishda, resurslarni mualliflik huquqlarini uzatishda foydalaniladi.

1.8. Bitkoin kriptovalyutasi

Bitkoin (inglizcha "Bitcoin" – so'zidan olingan, "bit" – bit va "coin" – tanga), bitimlarni ro'yxatga olish uchun bir xil nomdagi birlikdan foydalanadigan piring «peer-to-peer» to'lov tizimi. Tizimning ishlashi va himoyasini ta'minlash uchun kriptografik usullardan foydalaniladi, ammo shu bilan birga tizimda tranzaksiyalar haqidagi barcha ma'lumotlar ochiq matn shaklida saqlanadi.

Minimal uzatiladigan qiymat (kriptovalyutaning eng kichik o'lchov birligi) – 10^{-8} Bitkoin – Satoshi Nakamoto yaratuvchisi sharafiga "*satoshi*" deb nomlangan, garchi u o'zi ham bunday hollarda ba'zan «sent» so'zini ishlatgan bo'lsa ham.

Bitkoinni turlicha tavsiflashadi: *kriptovalyuta, virtual valyuta, raqamli valyuta, elektron pul.*

Ikki tomon o'rtasida tranzaksiyalar elektron to'lov vositachilarsiz amalga oshiriladi, bu operasiyani orqaga qaytarib bo'lmaydi. Tasdiqlangan tranzaksiyani bekor qilish mexanizmi yo'q (shu jumladan, to'lov noto'g'ri yoki mavjud bo'lmagan manzilga yuborilgan holatlarda ham, bitim boshqalarga ma'lum bo'lgan yopiq kalit bilan imzolangan holatlarda ham). Yopiq kalit egasi (yoki kalit ma'lum

bo'lgan boshqa shaxsdan tashqari) dan boshqa hech kimga mablag'larni vaqtincha bo'lsa ham to'sib qo'yish (hibsga olish) ning imkoni yo'q.

Bitkoinlarni ularni qabul qilishga rozi bo'lgan sotuvchilarning tovarlari yoki xizmatlariga almashtirish mumkin.

To'lovlarni amalga oshirish uchun to'lovchi tomonidan tranzaksiya yaratiladi. Tranzaksiyalar uchun komissiya qiymati to'lovchi tomonidan ixtiyoriy miqdorda belgilanadi, komissiya miqdori tranzaksiyani taqdiqlash jarayonida ustuvorlikka erishishda xizmat qiladi. Tranzaksiya tasdiqlamaguncha to'lov o'tgan deb hisoblanmaydi. Odatda, mijoz dasturi komissiyaning tavsiya etilgan miqdorini taklif qiladi. Komissiyasiz tranzaksiyalarni amalga oshirish mumkin va ularni qayta ishlash ham mumkin, ammo tavsiya etilmaydi, chunki tranzaksiyani tasdiqlash muddati noma'lum va juda uzoq bo'lishi ham mumkin.

Ikki martalik sarf-xarajatlar muammosi. Bitkoin nafaqat ikki martalik sarf-xarajatlar muammosini hal qildi, balki yana ko'plab afzalliklarni taqdim etadi. Ta'kidlash joizki, bunday afzalliklardan biri bu bitimlarning anonimligidir. Masalan, tizimni yaratgan va unda bir nechta tanga yasagan Satoshi butun dunyoga mutlaqo noma'lumligicha qolmoqda.

Aslida, Satoshi bitta shaxsmi yoki bir nechta odamlar guruhimi, bilmaymiz. Google, Satoshiga tegishli Bitkoinlarning qiymati 19,4 milliard dollarni tashkil etganligini aniqladi. Bu pullar hali ham hech kim tomonidan ishlatilmay turibdi.

Ma'lumki, bank barcha tranzasksiyalar haqidagi ma'lumotlar yozilgan daftarni (elekton ma'lumotlar bazasi) yuritadi. Bunday daftarlar jismoniy shaxslar, yuridik shaxslar va bank tomonidan to'ldirilib boriladi. Satoshi ushbu daftarni jamoatchilikka ochiq bo'lishini va jamoat tomonidan qo'llab-quvvatlanishini taklif qildi.

Bunday daftarni nashr qilganingizda (hammaga oshkor qilganda), sizga bir nechta fikrlar kelishi mumkin. Hech kim o'z yozuvlarini o'zgartira olmasligi uchun ushbu reyestr ruxsatsiz o'zgartirishlardan himoyalangan bo'lishi kerak. Daftardagi har bir yozuv jamoatchilikka ochiq bo'lganligi sababli, biz qanday qilib anonim