

***OLIY VA O'RTA MAHSUS TA'LIM VAZIRLIGI  
MIRZO ULUG'BEK NOMIDAGI UZBEKISTON MILLIY  
UNIVERSITETI***

**R.H. AYUPOV, A.V. KABULOV**

**KRIPTOGRAFIYA VA KRIPTOVALYUTALAR**

**Toshkent - 2018**

***R.H. Ayupov, A.V. Kabulov. Kriptografiya va kriptovalyutalar. T.: M. Ulug'bek nomidagi UzMU, 2018, 144 bet.***

## **ANNOTATSIYA**

Ushbu o'quv-uslubiy qo'llanma hozirgi paytda tezkorlik bilan rivojlanayotgan va bir qancha shov-shuvlarga sabab bo'layotgan raqamli valyutalar sohasiga va kriptovalyutalar bozoriga bag'ishlangan. Unda raqamli valyuta bozorining asosi bo'lgan kriptografiya va kriptoanaliz bilan bog'liq masalalar, kriptografiyadan kriptovalyutalarga o'tish mexanizmi, kriptografiyaning muhim elementi bo'lgan xeshlashtirish funktsiyalari haqida bir qancha ma'lumotlar berilgan. Undan so'ng, kriptografiyadan raqamli valyutalarga o'tish mantiqi tushuntirilib, kriptovalyutalarning asosiy turlari va ularning xossalari tushuntirilib o'tilgan. Turli hildagi loyihalarga investitsiyalar jalb qilish uchun ishlatiladigan **ICO** haqida tushuncha berilgan va uning mohiyati ko'rsatilgan. Kriptovalyutalar bozorida ishlashni istovchilar uchun esa ularni qanday qilib sotib olish va ular vositasida turli xildagi operatsiyalarni amalga oshirish texnologiyalari tushuntirib berilgan hamda bunda ishlatiladigan dasturiy-texnik vositalar ko'rsatib o'tilgan. Risola oxirida kriptovalyutalar bo'yicha bir qancha savollarga javoblar va glossariy berilganki, ular yordamida bu sohani yanada chuqurroq o'rganish mumkin bo'ladi. O'quv-uslubiy qo'llanma oliy ta'limning bakalavr va magistr mutahassisliklarida information texnologiyalar sohasida ta'lim olayotgan talabalarga tavsiya etilib, shu yo'nalishda tadqiqot ishlari olib borayotgan ilmiy xodimlarga va kriptovalyuta sohasidagi innovatsiyalar bilan qiziqqan barcha tadbirkorlik sub'ektlari foydalanishi uchun mo'ljallangan. Oshbu o'quv-uslubiy qo'llanma M. Ulug'bek nomidagi O'zbekiston Milliy Universiteti "*Matematik modellashtirish va kriptoanaliz*" kafedrasida muhokama qilingan va O'zMU Uslubiy Kengashining 2018 yil 12 dekaqbridagi 3-sonli majlisida ko'rib chiqilgan va nashrga tavsiya etilgan.

## MUNDARIJA

<b>K I R I S H</b> .....	<b>4</b>
<b>1. Kriptografiya va uning ahamiyati</b> .....	<b>7</b>
<b>2. Ma'lumotlarning electron himoyasi</b> .....	<b>22</b>
<b>3. Elektron imzo va xesh-funktsiyalar</b> .....	<b>28</b>
<b>4. Kriptoalyutalarning tarixi</b> .....	<b>37</b>
<b>5. Turli kriptoalyutalar va ularning tavsifi</b> .....	<b>44</b>
<b>6. Kriptoalyutalardan foydalanish muammolari</b> .....	<b>54</b>
<b>7. Blokcheynlar hamda ICO ning iqtisodiyotda ishlatilishi</b> .....	<b>58</b>
<b>8. Kriptoalyutalarning investitsiyalardagi ahamiyati</b> .....	<b>68</b>
<b>9. Kriptoalyutalar bozorida ishlash tamoillari</b> .....	<b>75</b>
<b>10. Kriptoalyuta birjalarida ishlash</b> .....	<b>91</b>
<b>11. Kriptoalyutalar bozorining rivojlanishi</b> .....	<b>109</b>
<b>12. Kriptoalyutalar bilan qanday ishlanadi</b> .....	<b>122</b>
<b>Hulosa va takliflar</b> .....	<b>127</b>
<b>Glossariy</b> .....	<b>132</b>
<b>Adabiyotlar ruyhati</b> .....	<b>141</b>

## K I R I S H

Diqqatingizga havola etilayotgan ushbu o'quv-uslubiy qo'llanmada ko'rib chiqiladigan masalalarni yoritishdan avval prezidentimiz tomonidan innovatsiyalar haqida aytilgan quyidagi so'zlarni eslatib o'tishni joiz deb hisoblaymiz: *“Xalqimiz dunyoqarashida innovatsiya muhitini yaratish eng muhim vazifamizdir. Innovatsiya bo'lmas ekan, hech bir sohada raqobat, rivojlanish bo'lmaydi. Bu sohadagi o'zgarishlarni xalqimizga keng targ'ib qilmasak, odamlarda ko'nikma paydo qilmasak, bugungi davr shiddati, fan-texnikaning mislsiz yutuqlari bilan hamqadam bo'lolmaymiz“*. Prezidentimiz tashabbusi bilan mamlakatimizda yetakchi soha va tarmoqlarni innovatsion rivojlantirish, innovatsion g'oyalar va texnologiyalarni ishlab chiqarishga keng joriy qilish yuzasidan izchil ishlar amalga oshirilmoqda. Davlatimiz rahbarining 2017 yil 29 noyabridagi *"O'zbekiston Respublikasi Innovatsion rivojlanish vazirligini tashkil etish to'g'risida"* gi farmoni bu boradagi ishlarni yangi bosqichga ko'tarishga xizmat qiladi. Mamlakatimizda ilmiy-tadqiqot va innovatsion faoliyatning istiqbolli yutuqlarini targ'ib qilish, bu borada samarali mexanizmlarni ishlab chiqish, ilmiy-experimental ixtisoslashgan laboratoriyalar, ilmiy-texnologik markazlar, texnoparklar va boshqa turdagi innovatsion tuzulmalarni mustahkamlash va rivojlantirish yangi vazirlikning asosiy faoliyat yo'nalishlaridandir. Bu sohadagi barcha yangiliklar va o'zgarishlarni tushunarli va qiziqarli ko'rinishda ommaviy axborot vositalari orqali halqimizga keng targ'ib qilmasak hamda insonlarda bu borada ko'nikmalar paydo qilmasak, bugungi information jamiyatning va unga mos davrning shiddati, fan-texnika va zamonaviy texnologiyalarning mislsiz yutuqlari bilan hamqadam bo'la olmaymiz. Xuddi shuning uchun ham bu sohada yangi ilmiy va ilmiy-ommabop adabiyotlar yaratish zamonaning eng muhim talablaridan biri bo'lib qolmoqda. Ushbu risolani ham ana shu muammoni hal qilishga bo'lgan urinishlardan biri deb hisoblashimiz mumkin.

Hozirgi zamonda tez sur'atlar bilan rivojlanayotgan internet biznesining asosiy turlaridan biri – kriptovalyutalar bilan amalga oshiriladigan turli xildagi moliyaviy operatsiyalar bo'lib, ularda faol va ishning ko'zini bilgan xolda ishtirok etish uchun ularning ma'no-mohiyatini bilish va to'la tushunish juda muhimdir. Shuni ta'kidlash kerakki, kriptovalyutalar bilan ishlashning boshqalaridan asosiy farqi – ularning tuzilmasi tarqoq (*markazlashmagan*) xoldaligidir. Kriptovalyutalar tizimida biror bir yagona markaz yoki bank mavjud emas va barcha tarmoq **R2R** kurinishidiga **pirring** arxitekturasida asosida ishlaydi. Ya'ni, bunday tarmoq bir huquqqa ega bo'lgan mijoz dasturlaridan iborat. Kriptovalyutaning har bir mijoz dasturi, o'z navbatida, o'z-o'zini ta'minlovchi tuzilmadan iborat bo'lib, ular global kriptovalyuta tarmog'iga ulanadilar va sutkasiga 24 soat mobaynida batamom avtomatik ravishda ishlaydilar. Kriptovalyutalarning emissiyasi esa **mayning** (*ma'dan qidirib topish*) tamoili asosida amalga oshiriladi. «**Mayning**» – bu kompyuter tizimlarining hisoblash quvvatlarini kriptovalyutaning tranzaksiyalari zanjirini xosil qilish uchun ishlatilish jarayonidir. Bunda har bir blok qandaydir to'g'rilik kriteriyalariga hamda murakkablik darajasiga ega bo'lishi lozim. Buning uchun xeshlashtirish algoritmlaridan foydalaniladi. Shunday qilib, **maynerlar** bir vaqtning o'zida yangi kriptopullarni topadilar va kriptovalyutaning barcha mumkin bo'lgan turlardagi tranzaksiyalarini amalga oshiradilar. Agarda maynerlar o'z ishlarini to'xtatsalar, kriptovalyuta ham yuqolib ketadi. Eng katta miqdorda aylanadigan kriptovalyutalarning (*Bitcoin, Litecoin*) mayningi uchun hozirgi davrdagi oddiy shaxsiy kompyuterlarning resurslari yetarli bo'lmaydi. Shuning uchun ham **maynerlar** ёки «*fermalar*» deb ataluvchi juda katta hisoblash quvvatiga ega bo'lgan tezkor va quvvatli kompyuter stantsiyalaridan foydalanadilar. Kriptovalyutalar ularni qalbakilashtirishdan xeshlashtirish algoritmlari asosida himoyalanganlar va ularni rasshifrovka qilish (*himoyasini buzish*) hozirgi kunda amaliy jihatdan mumkin emas. Ushbu masalaga biroz oydinlik kiritish uchun orqaga qaytamiz va buning uchun avvalo pul o'zi nima – degan savolga javob beramiz: Pul – biror bir mamlakatning yoki kelishuv asosida bir nechta davlatning tovar va hizmatlar oldi-sottisi uchun umumiy

ekvivalent sifatida qabul qilinadigan valyutasi bo'lib, u qog'oz, metal yoki electron ko'rinishda bugungi kun iqtisodiyotida amal qiladi. Valyutaning eng muhim jihatlaridan biri – unda emissiya qiluvchi (*pul chiqaruvchi*) biror bir muassasa (*O'zbekistonda Markaziy bank*) belgilanadi va tegishli qonunlarga muvofiq to'lovlarda belgilangan hududlarda o'z qiymatida qabul qilinishi qat'iy belgilanadi. Bugungi kundagi pullar *fiat* pullar (*nominal qiymati real qiymatidan katta farq qiladigan pullar*) hisoblanib, ularni muomalaga chiqarish uchun sarflanadigan harajatlar odatda pul ustida ko'rsatilgan qiymatdan ancha arzon bo'ladi. Masalan, AQSH da 100 dollarlik bitta kupyurani chiqarish uchun atigi 14 tsentlik harajat ketadi. Agar yarim asr oldin pullarning qiymati oltin ekvivalenti bilan ta'minlangan bo'lsa, xozirgi kunga kelib, ular mamlakatda yaratilgan mahsulot va xizmatlar umumiy yig'indisi bilan ta'minlanishi belgilangan. Biroq, naqdsiz pullar bilan amalga oshiriladigan har bir tranzaksiya (*pul o'tkazishlar amaliyoti*) bevosita biror bir moliya muassasasi orqali amalga oshirilishi yo'lga qo'yilgan. Bunda o'ziga hos nazorat yo'lga qo'yilgan bo'lib, havfsizlik va ko'rsatilgan xizmatlar uchun moliyaviy vositachilar (*banklar, birjalar va boshqalar*) komission haq olishi belgilangan. To'g'ri, naqd pul bilan hech qanday haq to'lamasdan ham to'g'ridan-to'g'ri to'lovlarni amalga oshirish mumkin, ammo bu amal yirik bitimlarda va uzoqdagi hamkorlar bilan amalga oshiriladigan to'lovlar uchun juda noqulay hisoblanadi. Buning ustiga, naqd pullarning qalbaki bo'lib chiqishi ehtimoli ham bor albatta. Yigirma birinchi asr axborot texnologiyalari asri bo'lgani uchun komp'yuter va internet texnologiyalari shiddat bilan rivojlanishi oqibatida to'lovlarni mukammallashtirish va yanada osonlashtirish ustida bir qancha ishlar amalga oshirildi. Diqqatingizga havola etilayotgan ushbu risola yuqorida qisqacha ravishda tavsif etilgan xuddi shu va shunga o'xshash masala va muammolari ommabop ravishda taqdim etishga va imkoniyat darajasida o'rganishga bag'ishlangan.

## ***1. Kriptografiya va uning ahamiyati***

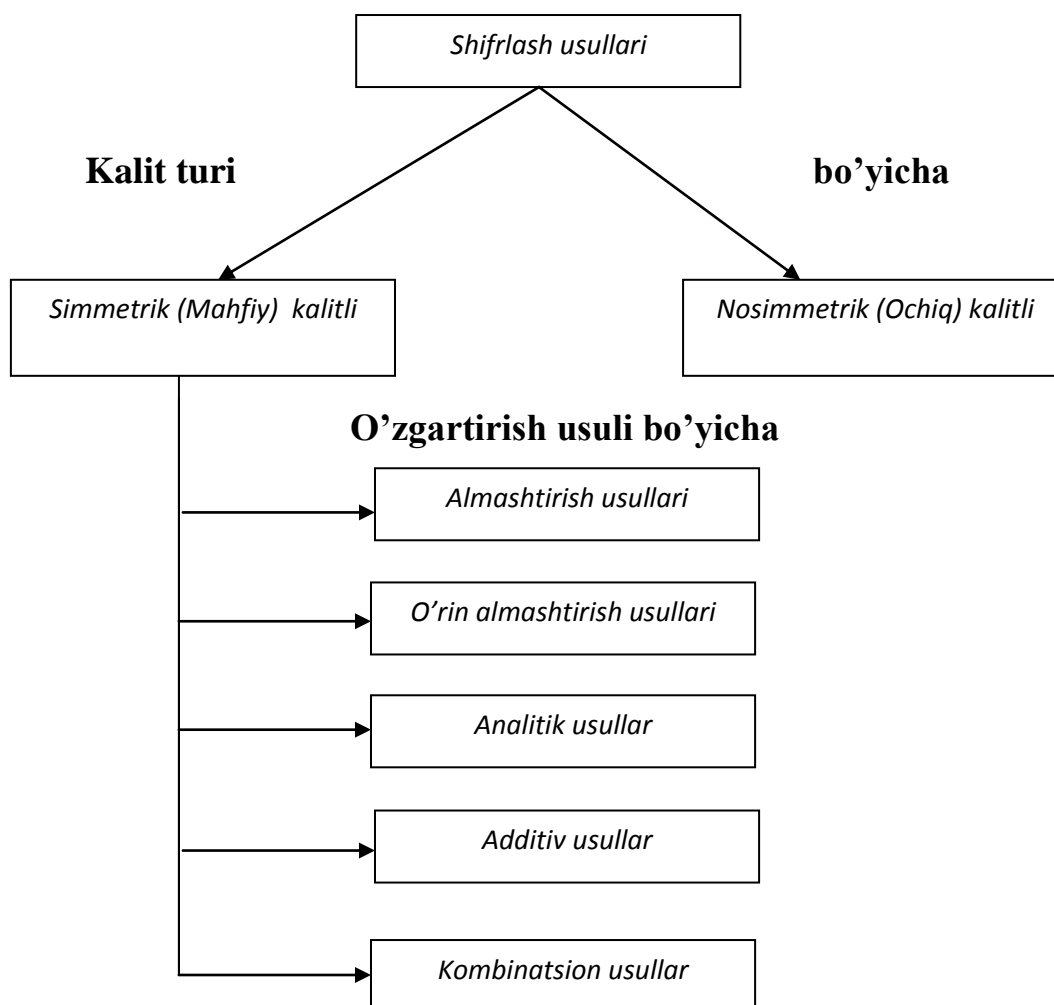
Grek tilidan tarjima qilganda kriptografiya so'zi "*mahfiy yozuv*" ma'nosini anglatadi. Kriptografiyaning klassik masalasi qandaydir boshlang'ich matnni (*ochiq matnni*) qandaydir qoidalar yordamida shifrlangan ko'rinishga o'tkazishdir. Bunda qandaydir belgilarning tasodifiyga o'xshagan ketma-ketligi shiromatn yoki kriptogramma deb ataladi. Ochiq matnni oddiy inson tomonidan tushunarsiz xolatga o'tkazish jarayoni fan tili bilan shifrlash yoki deshifrlash atamaları bilan ham nomlangan. Shifrlash deganda barcha tomonidan tushuniladigan va ochiq ma'lumotlarni shifrlangan ma'lumotlarga (*shifrlangan matnga*) o'zgartirishga aytilsa, deshifrlash deganda shifrlangan ma'lumotlarni ochiq ma'lumotlarga o'zgartiruvchi teskari jarayonga aytiladi. Shifrlash usuli (*shifr*) deb, shifrlash algoritmiga binoan ochiq informatsiyani berkitilgan (*tushunarsiz*) informatsiyaga o'zgartiruvchi amallar majmuasiga aytiladi. Ko'pchilik shifrlash tizimlari vaqtning beshavqat sinovlariga dosh bera olmadi, boshqalaridan esa xozirgi davrgacha foydalaniladi. Hisoblash mashinalari, komp'yuter tarmoqlari va internetning paydo bo'lishi ma'lumotlarni shifrlash-deshifrlashning ko'pgina yangi usullarining yaratilishiga turtki bo'ldi. Shifrga xujum (*yoki kriptoolaliz*) kalitni bilmasdan turib, shifrlash algoritmini aniqlashga va berk bo'lgan imformatsiyani beruxsat o'qishga (*rasshifrovka qilishga*) bo'lgan urinishdir.

*Shifrlashning zamonaviy usullari quyidagi talablarga javob berishi lozim:*

- Shifrnig kriptoolalizga (*deshifrovkaga*) bo'lgan turg'unligi (*chidamliligi – kriptoturg'unlik*) shunday bo'lishi lozimki, uning fosh etilishi faqatgina kalitlarning to'liq saralash masalasini yechish orqaligina amalga oshirilishi mumkin bo'lsin;
- Kriptoturg'unlik shifrlash algoritmining mahfiyligi orqali emas, balki kalitning mahfiyligi orqali ta'minlanadi;
- Shifr matn hajmi bo'yicha dastlabki informatsiyadan ortiq bo'lmasligi lozim;

- Shifrlashdagi xatoliklar informatsiyaning buzilishiga va yo'qolishiga olib kelmasligi kerak;
- Shifrlash vaqti juda ham katta bo'lmasligi zarur;
- Shifrlashning narxi berkitiluvchi informatsiya narxi bilan muvofiqlashtirilishi lozim.

Shifrlashning keng miqyosda ishlatiluvchi algoritmini amalda mahfiy saqlash mumkin emas. Shu sababli, algoritmnining kriptanalitik foydalanishi mumkin bo'lgan zaif tomonlari bo'lmasligi lozim. Agar bu shart bajarilsa, shifrnining kriptoturg'unligi kalit uzunligi orqali aniqlanadi, chunki shifrlangan informatsiyani fosh etishning yagona yo'li – kalit kombinatsiyalarini saqlovchi algoritmnini rasshifrovka qilishdir. Shunday qilib, kriptanaliz uchun sarf qilinadigan vaqt va vositalar kalit uzunligiga hamda shifrlash algoritmining murakkabligiga bog'liqdir. Shifrlash usullari turli alomatlari bo'yicha quyidagi chizmada keltirilgandek tasniflanishi mumkin:





### *Simmetrik (mahfiy) kalitli shifrlash tizimlari*

Almashtirish usullarining mohiyati – bir alfavitda yozilgan information simvollarni boshqa alfavit simvollari bilan ma'lum bit qoida bo'yicha almashtirishdan iboratdir. Bu guruhga mansub eng sodda usul sifatida **to'g'ridan-to'g'ri almashtirish usulini** ko'rsatish mumkin. Dastlabki informatsiya yoziluvchi  $A_0$  alfavitning  $s_{0i}$  simvollariga shifrlovchi alfavitning  $s_{1i}$  simvoli mos qo'yiladi. Oddiy xolda ikkala alfavit ham bir xil simvollar to'plamiga ega bo'lishi mumkin. Ikkala alfavitdagi simvollar o'rtasidagi moslik ma'lum bir algoritm bo'yicha  $K$  simvollar uzunligiga ega bo'lgan dastlabki matn  $T_0$  simvollarining raqamli ekvivalentlarini o'zgartirish orqali amalga oshiriladi.

*Monoalfavitli almashtirish algoritmi quyidagi qadamlar ketma-ketligi ko'rinishida ifodalanishi mumkin:*

**1-qadam:**  $[1 \times R]$  o'lchamli dastlabki  $A_0$  alfavitdagi har bir simvol  $s_0 \in T(i=1, K)$  ni  $A_0$  alfavitdagi  $s_{0i}$  simvol tartib raqamiga mos keluvchi  $h_{0i}(s_{0i})$  soniga almashtirish yo'li bilan raqamlar ketma ketligi  $L_{0h}$  ni shakllantirish.

**2-qadam:**  $L_{0h}$  ketma-ketligining har bir sonini  $h_{1i} = (k_1 \times h_{0i}(s_{0i}) + k_2) \pmod R$  formula orqali hisoblanuvchi  $L_{1h}$  ketma ketligining mos soni  $h_{1i}$  ga almashtirish yo'libilan  $L_{1h}$  sonlar ketma ketligini shakllantirish, bu yerda  $k_1$  o'nlik koeffitsient,  $k_2$  esa siljitish koeffitsienti. Tanlangan  $k_1$  va  $k_2$  koeffitsientlar  $h_{0i}$  va  $h_{1i}$  sonlarining bir ma'noli mosligini ta'minlashi lozim.  $h_{1i} = 0$  deb olinganida  $h_{1i} = R$  almashinuvi bajarilishi kerak.

**3-qadam:**  $L_{1h}$  ketma ketligining har bir soni  $h_{1i}(s_{1i})$  ni  $[1 \times R]$  o'lchamli shifrlash alfavitining mos  $s_{1i} \in T_1(i=1, K)$  simvoli bilan almashtirish orqali  $T_1$  shifr matnini hosil qilish.

**4-qadam:** Olingan shifr matni o'zgarmas  $b$  uzunlikdagi bloklarga ajratiladi. Agar oxirgi blok to'liq bo'lmasa, blok orqasiga mahsus simvol-to'ldirgichlar joylashtirish (masalan, \* simvolini).

**Misol:** Shifrlash uchun dastlabki ma'lumotlar:

AYUPOV R.H., KABULOV V.K.

$T_0 = \langle \text{ХИМОЯ\_ХИЗМАТИ} \rangle$

$A_0 = \langle \text{АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЭЮЯЎҚҒҲ} \rangle$

$A_1 = \langle \text{ОРЁЬЯТЭ-ЖМЧХАВДЙФҚКСЕЗПИЦГҲЛЫШБУЮ ҚҒН} \rangle$

$R=36 \quad k_1=3 \quad k_2=15 \quad b=4$

Algoritmnining qadamba-qadam bajarilishi quyidagi natijalarga olib keladi:

**1-qadam:**  $L_{0h} = \langle 35, 10, 14, 16, 31, 36, 23, 10, 9, 14, 1, 20, 10 \rangle$

**2-qadam:**  $L_{1h} = \langle 12, 9, 21, 17, 36, 14, 12, 9, 6, 21, 18, 3, 9 \rangle$

**3-qadam:**  $T_1 = \langle \text{ХЖЕФНВХЖТЕҚЁЖ} \rangle$

**4-qadam:**  $T_1 = \langle \text{ХЖЕФ НВХЖ ТЕҚЁЖ***} \rangle$

Rasshifrovka qilishda bloklar birlashtirilib,  $K$  simvolli shifromatn  $T_1$  hosil qilinadi. Rasshifrovka qilish quyidagi butun sonli tenglamani (tselochislennoe uravnenie) yechish kerak bo'ladi:

$$k_1 h_{0i} + k_2 = n R + h_{1i}$$

Ushbu tenglamadagi  $k_1$ ,  $h_{1i}$ ,  $k_2$  va  $R$  butun sonlar ma'lum bo'lganda  $h_{0i}$  kattaligi  $n$  ni saralash orqali hisoblanadi. Bu muolajani shifromatnning barcha simvollariga tadbiq qilish uning rasshifrovka qilinishiga olib keladi. Almashtirish usulining kamchiligi sifatida dastlabki va berilgan matnlar statistik ko'rsatkichlarining bir xilligini ko'rsatish mumkin. Dastlabki matn qaysi tilda yozilganini bilgan xolda, kriptanalitik axborotlarni statistik qayta ishlab, ikkala alfavitdagi simvollar orasidagi mos kelishliklarni aniqlashi va matnni rasshifrovka qilishi mumkin

### ***Polialfavitli almashtirish usullari***

Bu usullar yetarlicha yuqori darajadagi kriptoturg'unlikka ega va bunda dastlabki matn simvollarini almashtirish uchun bir necha alfavitlardan foydalanadilar. Rasman polialfavitli almashtirishni quyidagihca tasavvur qilish mumkin.  $N$  – alfavitli almashtirishda dastlabki  $A_0$  alfavitdagi  $s_{0i}$  simvoli  $A_1$  alfavitdagi  $s_{1i}$  simvoli bilan almashtiriladi va hakozi.  $s_{0N}$  simvolini  $s_{NN}$  simvoli bilan almashtirgandan so'ng  $s_{0(N+1)}$  simvolining o'rnini  $A_1$  alfavitdagi  $s_{1(N+1)}$  simvoli oladi va hakozi.

Polialfavitli almashtirish algoritmlari ichida **Viginer jadvali (matritsasi)**  $T_b$  ni ishlatuvchi algoritm eng keng miqyosda tarqalgan. **Viginer jadvali**  $[R \times R]$  o'lchamli kvadrat matritsadan iborat bo'lib ( $R$  - ishlatilayotgan alfavitdagi simvollar soni), birinchi qatorda simvollar alfavit tartibida joylashtiriladi. Ikkinchi qatordan boshlab, simvollar chapga bitta o'ringa siljirilgan xolda yoziladi. Siqib chiqarilgan simvollar o'ng tarafdagi bo'shagan o'rinni to'ldiradi (tsiklik siljitish). Agar bu jarayonda kirill alfavitidagi o'zbek alfaviti ishlatilsa, **Viginer matritsasi** quyida keltirilganidek, **(36x36)** o'lchamga ega bo'ladi:

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЭЮЯЎҚҒҲ\_  
 БВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЭЮЯЎҚҒҲ\_А  
 ВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЭЮЯЎҚҒҲ\_АБ  
 ГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЭЮЯЎҚҒҲ\_АБВ  
 ДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЭЮЯЎҚҒҲ\_АБВГ  
 ЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЭЮЯЎҚҒҲ\_АБВГД  
 ЁЖЗИЙКЛМНОПРСТУФХЦЧШЭЮЯЎҚҒҲ\_АБВГДЕ  
 .....  
 .....  
 .....  
 \_АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЭЮЯЎҚҒҲ

Shifrlash takrorlanmaydigan  $M$  simvoldan iborat kalit yordamida amalga oshiriladi. Viginerning to'liq matritsasidan  $[(M+1), R]$  o'lchamli shifrlash matritsasi  $T_m$  ajratiladi. Bu matritsaning birinchi qatori va birinchi elementlari kalit simvollariga mos keluvchi qatorlardan iborat bo'ladi. Agar kalit sifatida **<ҒЎЗА>** so'zi tanlangan bo'lsa, shifrlash matritsasi  $T_m$  quyidagi beshta qatordan iborat bo'ladi:

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЭЮЯЎҚҒҲ\_  
 ҒҒ\_АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЭЮЯЎҚ  
 ЎҚҒҲ\_АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЭЮЯ  
 ЗИЙКЛМНОПРСТУФХЦЧШЭЮЯЎҚҒҲ\_АБВГДЕЁЖ  
 АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЭЮЯЎҚҒҲ\_

**Viginer jadvali** yordamida shifrlash algoritmi quyidagi qadamlar ketma ketligidan iborat:

**1-qadam:** Uzunligi  $M$  simvolli  $K$  kalitni tanlash.

**2-qadam:** Tanlangan  $K$  kalit uchun  $[(M+1), R]$  o'lchamli shifrlash matritsasi

$T_m = (b_{ij})$  ni qurish.

**3-qadam:** Dastlabki matnning har bir simvoli  $s_{0R}$  tagiga kalit simvoli  $k_m$  joylashtiriladi. Kalit kerakli miqdorda takrorlanadi.

**4-qadam:** Dastlabki matn simvollar shifrlash matritsasi  $T_m$  dan quyidagi qoida bo'yicha tanlangan simvollar bilan quyidagicha tartibda ketma ket almashtiriladi:

1.  $K$  kalitning almashtiriluvchi  $s_{0R}$  simvoliga mos  $k_m$  simvoli aniqlanadi.
2. Shifrlash matritsasi  $T_m$  dagi  $k_m = b_{ij}$  shart bajariluvchi  $i$  qator topiladi.
3.  $s_{0R} = b_{ij}$  shart bajariluvchi  $j$  ustun aniqlanadi.
4.  $s_{0R}$  simvoli  $b_{ij}$  simvoli bilan almashtiriladi.

**5-qadam:** Shifrlangan ketma-ketlik ma'lum uzunlikdagi (masalan, 4 simvolli) bloklarga ajratiladi.

*Matnni rasshifrovka qilish esa quyidagicha ketma ketlikda amalga oshiriladi:*

**1-qadam:** Shifrlash algoritmining uchinchi qadamidagidek, shifroformat tagiga kalit simvollar ketma ketligi yoziladi.

**2-qadam:** Shifromatndan  $s_{1R}$  simvollar va mos kalit simvollar  $k_m$  ketma ket tanlanadi. Shifrlash matritsasi  $T_m$  dagi  $k_m = b_{ij}$  shartni qanoatlantiruvchi  $i$  qator aniqlanadi.  $i$  qatorda  $b_{ij} = s_{1R}$  element aniqlanadi. Rasshifrovka qilingan matnda  $r$  -o'rniga  $b_{ij}$  simvoli joylashtiriladi.

**3-qadam:** Rasshifrovka qilingan matn ajratilmasdan yoziladi. Xizmatchi simvollar esa olib tashlanadi.

### **Мисол:**

$K = \langle F\ddot{U}3A \rangle$  kaliti yordamida  $T = \langle \Pi A X T A \_ F A P A M H \rangle$  dastlabki matnni shifrlash va so'ngra rasshifrovka qilish talab etilsin. Shifrlash va rasshifrovka qilish natijalari quyida keltirilgan:

*Dastlabki matn:*  **$\Pi A X T A \_ F A P A M H$**

**Kalit: FŶZAFŶZAFŶZA**

**Almashtirilgan so'nggi matn: MŶЯTFЯEAHŶΦИ**

**Shifromatn: MŶЯT FЯEA HŶΦИ**

**Kalit: FŶZA FŶZA FŶZA**

**Rasshifrovka qilingan matn: ПAXTA \_FAPAMИ**

**Dastlabki matn: ПAXTA \_FAPAMИ**

Polialfavitli almashtirish usullarining kriptoturg'unligi oddiy almashtirish usullariga nisbatan sezilarli darajada yuqori, chunki ularda dastlabki ketma ketlikning bir simvollari turli simvollar bilan almashtirilishi mumkin. Ammo shifrnining statistik usullarga bardoshliligi kalit uzunligiga bog'liq.

### ***O'rin almashtirish usullari***

O'rin almashtirish usullariga binoan dastlabki matn belgilangan uzunlikdagi bloklarga ajratilib, har bir blok ichidagi simvollar o'rni ma'lum algoritim bo'yicha almashtiriladi. Eng oson o'rin almashtirishga misol qilib, dastlabki informatsiya blokini matritsaga qator bo'yicha yozishni, o'qishni esa ustun bo'yicha amalga oshirishni ko'rsatish mumkin. Matritsa qatorlarini to'ldirish va shirflangan informatsiyani ustun bo'yicha o'qish ketma-ketligi kalit yordamida bajarilishi mumkin. Usulning kriptoturg'unligi blok uzunligiga (*matritsa o'lchamiga*) bog'liq. Masalan, uzunligi 64 simvolga teng bo'lgan blok (*matritsa o'lchami 8x8*) uchun kalitning 1,6 milliard kombinatsiyasi bo'lishi mumkin. Uzunligi 256 simvolga teng bo'lgan blok (*matritsa o'lchami 16x16*) uchun esa kalitning mumkin bo'lgan kombinatsiyalari soni  $1,4 \cdot 10^{26}$  ga yetishi mumkin. Bu xolda kalitni saralash masalasi zamonaviy komp'yuterlar uchun ham murakkab amal hisoblanadi.

***Gamil'ton marshrutlariga asoslangan usulda*** ham o'rin almashtirishlardan foydalaniladi. Ushbu usul quyidagi qadamlarni bajarish orqali amalga oshiriladi:

***1-qadam:*** Dastlabki informatsiya bloklarga ajratiladi. Agar shifrlanuvchi informatsiya uzunligi blok uzunligiga karrali bo'lmasa, oxirgi blokda bo'sh o'rinlarga mahsus xizmatchi simvollar – to'ldiriluvchilar joylashtiriladi. Masalan, \* simvoli.

**2-qadam:** Blok simvollari yordamida jadval to'ldiriladi va bu jadvalda simvolning tartib raqami uchun ma'lum bir joy ajratiladi.

**3-qadam:** Jadvaldagi simvollarni o'qish marshrutlarning biri bo'yicha amalga oshiriladi. Marshrutlar sonining oshishi shifr kriptoturg'unligini oshiradi. Marshrutlar ketma-ket tanlanadi yoki ularning navbatlanishi kalit yordamida beriladi.

**4-qadam:** Simvollarning shifrlangan ketma-ketligi belgilangan  $L$  uzunlikdagi bloklarga ajratiladi.  $L$  kattalik birinchi qadamda dastlabki informatsiya bo'linadigan bloklar uzunligidan farqlanishi mumkin

**Ma'lumotlarni rasshifrovka qilish** esa teskari tartibda amalga oshiriladi. Kalitga mos xolda marshrut tanlanadi va bu marshrutga binoan jadval to'ldiriladi. Jadvaldan simvollar element nomerlari kelishi tartibida o'qiladi.

**Misol:**

Dastlabki matn  $T_0 = \langle \text{ЎРИН АЛМАСТИРИШИ USULI} \rangle$  ni shifrlash tilan etilsin. Kalit va shifrlangan bloklar uzunligi mos xolda quyidagilarga teng:

$$K = \langle 2, 1, 1 \rangle \quad L = 4$$

Shifrlash uchun mahsus jadval va ikkita marshrutdan foydalaniladi. Berilgan shartlar uchun matritsalar to'ldirilgan marshrutlar grafik ko'rinishda ifodalanadi. Amaliyotda o'rin almashtirish usulini amalga oshiruvchi mahsus shifrovchi va deshifrovchi apparat vositalari ishlatiladi.

O'rin almashtirish usullarining amalga oshirishi sodda bo'lsada, ular ikkita jiddiy kamchiliklarga ega. Birinchidan, bunday shifrlashni statistic usullar yordamida fosh qilish mumkin. Ikkinchidan, agar dastlabki matn uzunligi  $K$  simvollaridan tashkil topgan bloklarga ajratilsa, shifrnı fosh qilish uchun shifrlash tizimiga bittasidan boshqa barcha simvollari bir xil bo'lgan matn informatsiyasining  $K-1$  blogini yuborish kifoya.

***Shifrlashning analitik usullari***

Matritsa algebrasiga asoslangan shifrlash usullari eng ko'p tarqalgan. Bunda dastlabki informatsiyaning  $B_k = (b_j)$  vector ko'rinishida berilgan  $k$  – blokni shifrlash  $A = (a_{ij})$  matritsa kalitni  $B_k$  vektorga ko'paytirish orqali amalga

AYUPOV R.H., KABULOV V.K.

oshiriladi. Natijada  $C_k = (c_i)$  vector ko'rinishigan shifromatn bloki hosil qilinadi. Bu vektorning elementlari  $c_i = \sum_j a_{ij}b_j$  ifodasi orqali aniqlanadi. Informatsiyani rasshifrovka qilish  $C_k$  vektorlarni  $A$  matritsaga teskari bo'lgan  $A^{-1}$  matritsaga ketma-ket ko'paytirish orqali aniqlaniladi.

### *Shifrlashning additiv usullari*

Shifrlashning additiv usullariga binoan dastlabki informatsiya simvollariga mos keluvchi raqam kodlarining ketma-ketligi **gamma** deb ataluvchi qandaydir simvollar ketma-ketligiga mos keluvchi kodlar ketma-ketligi bilan ketma-ket jamlanadi. Shu sababli, shifrlashning additiv usullari *gammalsh* deb ham ataladi. Ushbu usullar uchun kalit sifatida **gamma** ishlatiladi. Additiv usullarning kriptoturg'unligi kalit uzunligiga va uning statistic ko'rsatgichlarining tekisligiga bog'liq. Agar kalit shifrlanuvchi simvollar ketma-ketligidan qisqa bo'lsa, shifromatn kriptoolitik tomonidan statistic usullar yordamida rasshifrovka qilinishi mumkin. Kalit va dastlabki informatsiya uzunliklari qanchalik farq qilsa, shifromatnga muvaffaqiyatli hujum ehtimolligi ham shunchalik ortadi. Agar kalit uzunligi shifrlanuvchi informatsiya uzunligidan katta bo'lgan tasodifiy sonlarning davriy bo'lmagan ketma-ketligidan iborat bo'lsa, kalitni bilmasdan turib, shifromatnni rasshifrovka qilish amaliy jihatdan mumkin emas. Amaliyotda asosini psevdotasodifiy sonlar generatorlari (yoki *datchiklari*) tashkil etgan additiv usullar eng ko'p tarqalgan va samarali hisoblanadi. Bunday generatorlar psevdotasodifiy sonlarning cheksiz ketma-ketligini shakllantirishda nisbatan qisqa uzunlikdagi dastlabki informatsiyadan foydalaniladi. Psevdotasodifiy sonlar ketma-ketligini shakllantirishda kogruent generatorlardan ham foydalaniladi. Bu toifaga mansub generatorlar sonlarning shunday psevdotasodifiy ketma-ketliklarini shakllantiradiki, ular uchun generatorlarning davriyligi va chiqish yo'li ketma-ketliklarining tasodifiyligi kabi asosiy ko'rsatgichlarini qat'iy matematik tarzda ifodalash mumkin. Bunday generatorlarni apparat yoki dasturiy vositalar yordamida osonlik bilan yaratish mumkin.

### ***Shifrlashning kombinatsiyalangan usullari***

Qudratli komp'yutarlar, tarmoq texnologiyalari va neyronli hisoblash tizimlarining paydo bo'lishi hozirgacha umuman fosh qilinmaydi deb hisoblabgan kriptografik tizimlarning o'brusizlantirilishiga sabab bo'ldi. Bu esa o'z navbatida yuqori turg'unlikka ega bo'lgan kriptotizimlarni yaratishni taqozo qildi. Bunday kriptotizimlarni yaratish usullaridan biri shifrlash usullarning kombinatsiyalangan tartibda qo'llanilishidir. Quyida eng kam vaqt sarf qilgan xolda kriptoturg'unlikni jiddiy ravishda oshirish imkonini beruvchi shifrlashning kombinatsiyalangan usuli haqida gap boradi. Shifrlashning ushbu kombinatsiyalangan usulida ma'lumotlarni shifrlash ikki bosqichda amalga oshiriladi. Birinchi bosqichda ma'lumotlar standart usul (*masalan, DES usuli*) yordamida shifrlansa, ikkinchi bosqichda shifrlangan ma'lumotlar ikkinchi bor mahsus usul bo'yicha qayta shifrlanadi. Mahsus usul sifatida ma'lumotlar vektorining elementlarini noldan farqli bo'lgan son matritsasiga ko'paytirishdan foydalanish mumkin. Gammalashni qo'llashda agar shifr gammasi sifatida raqamlarning takrorlanmaydigan ketma-ketligi ishlatilsa, shifrlangan matnni fosh qilish juda ham qiyin bo'ladi. Odatda shifr gammasi har bir so'z uzunligidan katta bo'lsa va dastlabki matnning hech qanday qismi ma'lum bo'lmasa, shifrnı faqat to'g'ridan-to'g'ri saralash orqaligina fosh qilish mumkin. Bunda kriptoturg'unlik kalit o'lchami orqali aniqlanadi. Shifrlashning bu usulida ko'pincha himoya tizimining dasturiy ko'rinishda amalga oshirilishida foydalaniladi va shifrlashning bu usuliga asoslangan tizimlarda bir sekunda ma'lumotlarning bir nacha yuz kilobaytini shifrlash imkoniyati mavjud. Rasshifrovka qilish jarayoni – kalit ma'lum bo'lganda, shifr gammasini qayta generatsiyalash va uni shifrlangan ma'lumotlarga singdirishdan iboratdir.

### ***Ochiq kalitli shifrlash tizimlari***

Ochiq kalitli shifrlash tizimlarida ikkita kalit ishlatiladi. Informatsiya ochiq kalit orqali shifrlansa, mahfiy kalit yordamida rasshifrovka qilinadi. Ochiq kalitli tizimlarni qo'llash asosida qaytarilmas yoki bir tomonli funktsiyalardan

AYUPOV R.H., KABULOV V.K.



foydalanish yotadi. Bunday funktsiyalar quyidagi xususiyatlarga ega. Hech kimga sir emaski,  $x$  ma'lum bo'lsa,  $y = f(x)$  funktsiyani aniqlash juda oson. Ammo  $y = f(x)$  funktsiyaning ma'lum qiymati bo'yicha  $x$  ni aniqlash amaliy jihatdan juda ham qiyin. Kriptografiyada yashirin deb ataluvchi yo'lga ega bo'lgan bir tomonli funktsiyalar ishlatiladi.  $z$  parametrli bunday funktsiyalar quyidagi xususiyatlarga ega. Ma'lum  $z$  parameter uchun  $E_z$  va  $D_z$  algoritmlarini aniqlash mumkin.  $E_z$  Algoritmi yordamida aniqlik sohasidagi barcha  $x$  lar uchun  $f_z(x)$  funktsiyani osongina olish mumkin. Xuddi shu tariqa  $D_z$  algoritmi yordamida joiz qiymatlar sohasidagi barcha  $y$  lar uchun teskari funktsiya  $x = f^{-1}(y)$  ham osongina aniqlanadi. Ayni vaqtda joiz qiymatlar sohasidagi barcha  $z$  parametrlar va deyarli barcha  $y$  uchun hatto  $E_z$  ma'lum bo'lganda ham  $x = f^{-1}(y)$  ni hisoblashlar yrdamida topib bo'lmaydi. Ochiq kalit sifatida  $y$  ishlatilsa, mahfiy kalit sifatida  $x$  ishlatiladi. Ochiq kalitni ishlatib, shifrlash amalga oshirilsa, o'zaro muloqotda bo'lgan sub'ektlar orasida mahfiy kalitni almashish zaruriyati yo'qoladi. Bu esa o'z navbatida uzatiluvchi informatsiyaning kriptohimoyasini soddalashtiradi. Ochiq kalitli kriptotizimlarni bir tomonlama funktsiyalar ko'rinishi bo'yicha farqlash mumkin. Bularning ichida **RSA**, **Эль-Гамал** va **Мак-Элис** tizimlarini aloxida tilga olish o'rinlidir. Xozirda eng samarali va keng tarqalgan ochiq kalitli algotirm sifatida **RSA** algoritmini ko'rsatish mumkin. Ushbu algoritmnning nomi uni yaratganlarning familiyalari birinchi harflaridan olingan (**R**ivest, **S**hamir, **A**dleman). Algoritm modul arifmetikasining darajaga ko'tarish amalidan foydalanishga asoslangan (*bunda Eyler funktsiyasi hisoblanadi*). **El-Gamal** tizimi chekli maydonlarda diskret logarifmlarning hisoblanish murakkabligiga asoslangan. **Мак-Элис** kriptotizimida esa xatoliklarni tuzatuvchi kodlar ishlatiladi.

*Xozirgi kunda shifrlashning zamonaviy usullari quyidagi talablarga javob berishi kerak:*

- Shifrnig kriptotizimga turg'unligi (*kriptoturg'unlik*) shunday bo'lishi lozimki, uning fosh etilishi faqatgina kalitlarni to'liq saralash masalasini yechish orqaligina amalga oshirilishi mumkin bo'lsin.

- Kriptoturg'unlik shifrlash algoritmining mahfiyligi orqali emas, balki kalitning mahfiyligi orqali ta'minlanadi.
- Shifrimatn hajmi bo'yicha dastlabki ma'lumotlardan ortiq bo'lmasligi kerak.
- Shifrlashdagi xatoliklar informatsiyaning buzilishiga va yo'qolishiga olib kelmasligi lozim.
- Shifrlash vaqti juda ham katta bo'lmasligi kerak.
- Shifrlash narxi berkitiluvchi informatsiya narxi bilan muvofiqlashtirilishi lozim.

Shifrlash usullariga bo'lgan ushbu talablar ruyhati tom ma'noda jo'natilayotgan axborotning tegishli qo'llarga (*tashkilot, individ yoki tarmoq komp'yuterlariga*) havfsiz darajada yetib borishini to'la-to'kis ta'minlab bertadi.

Endi esa quyida keltirilgan shifrlashga bag'ishlangan bir qancha testlarni o'rganib va yechib, mavzuni yanada puxtaroq o'zlashtirib oling.

## TESTLAR

*Eslatma: □ – quyida ushbu belgi bo'sh joy (probel) ni ko'rsatish uchun ishlatiladi.*

1. Axborotni kriptografik muhofazalash bilan qaysi fan shug'ullanadi?

- A) Kriptologiya
- B) Kriptografiya
- C) Kriptoanaliz
- D) Kriptotizim
- E) Kriptoshlyuz

2. Kriptografiya tizimi necha qismga bo'linadi?

- a) 2 ta – shifrlash va deshifrlash
- b) 2 ta – simmetrik va asimmetrik
- c) 4 ta – shifrlash, deshifrlash, simmetrik, asimmetrik
- d) 3 ta – simmetrik, asimmetrik, analitik
- e) Qismlarga bo'linmaydi.

3. «Viginer jadvali» ning o'lchami qanday bo'ladi?

- a)  $36 \times 36$
- b)  $26 \times 26$
- c)  $N \times M$  va foydalanilayotgan raqamlarga bog'liq
- d)  $R \times R$ , foydalanilayotgan alfavitlar soniga bog'liq
- e) To'g'ri javob yo'q.

5. «Gamilton marshruti» kriptografik tizimning qaysi usuliga kiradi?

- a) Asimmetrik usulga
- b) Additivlik usuliga
- c) Orin almashtirish usuliga
- d) Kombinatsiyalangan usulga
- e) Analitik usulga.

6. Shennon o'z sxemasini nechanchi yilda yaratgan?

- a) 1949 yilda
- b) 1959 yilda
- c) 1939 yilda
- d) 1969 yilda
- e) 1929 yilda

7. «Kriptoturg'unlik» nima?

- a) Qidirilayotgan kalitning mumkin bo'lgan barcha imkoniyatlari soni
- b) Matnni shifrlash yoki deshifrlash uchun zarur bo'lgan ma'lumot
- c) Ochiq matnni shifrlash yoki deshifrlash jarayoni
- d) Shifrlash va dehifrlash masalalariga tegishli bo'lgan alfavit ko'rinishi
- e) Shifrlash kaliti noma'lum bo'lgan xolda shifrlangan matnni

deshifrlashdagi qiyinchilik darajasi

8. Kriptoturg'unlikni belgilovchi ikkita ko'rsatgichni ko'rsating:

a) Shifrlash vaqti katta bo'lmasligi kerak, shifrlangan matn hajmi bo'yicha dastlabki axborotdan ortiq bo'lmasligi zarur.

b) Dehifrlash uchun zarur bo'lgan o'rtacha vaqt, deshifrlash uchun qidirilayotgan kalitlarning mumkin bo'lgan barcha imkoniyatlar soni

- c) Simmetrik kriptotizim, asimmetrik kriptotizim

d) Mavjud bo'lgan axborotlarni tashkillashtirish, ruxsat etilmagan axborotni beruxsat olmaslik

e) Ruxsat etilgan xolda foydalanuvchilarning vakolatlarini o'zgartirish

ж) Deshifrlash uchun zuru bo'lgan vaqt

10.  $N$  harfli almashtirishda dastlabki  $A_0$  alfavitdagi  $S_{0I}$  simvoli  $A_I$  alfavitdagi  $S_{II}$  simvoli bilan almashtiriladi va xakozo.  $S_{0N}$  ni  $S_{NN}$  simvolini almashtirishdan so'ng  $S_{0(N+I)}$  simvolining o'rnini  $A_I$  alfavitdagi  $S_{I(N+I)}$  simvoli oladi va xakozo. Ushbu almashtirish qaysi usulga tegishli deb o'ylaysiz?

- a) Additivlik usuli
- b) Analitik usul
- c) Yarim alfavitli almashtirish usuli
- d) To'g'ri javob yo'q
- e) Asimmetrik usul

11. O'rin almashtirish usuli orqali shifrlang:

$T_0 = \text{ХУР\_ЎЗБЕКИСТОН}$

$B = 4$

- a) ХУКО\_ЎЗИН\_РБС\*\_□ЕТ\*
- b) □РУХ\_ЕБЗУ\_ТСИК\_\*\*НО
- c) ХУК\_ОУЗ\_ИНР\_БС\*\_□ЕТ\_\*\*\*
- d) ХУР□\_УЗБЕ\_КИСТ\_ОН\*\*
- e) □РУХ\_ЕБЗУ\_ТСИК\_\*\*НО

12. «Аъло ўйинчи» so'zini «Sehrli kvadrat» usulidan foydalanib shifrlan. Bunda  $B = 4$  ga teng deb oling.

- a) Аоии\_ъун\*\_лйч\*
- b) Аъло\_\*\*уй\_ня\*\*\_□и\*\*
- c) о\*\*Анйу\*□ичи\*ъл\*
- d) Аоииъун\*лйч\*
- e) о\*\*А\_нйу\*\_□ичи\_\*ъл\*

13. **иен\_нмн\_□иу\_гие\_мтт\_сеи\_рв** - Ushbu shifrlangan matnni «Ikki marta qo'yish usuli» yordamida deshifrlang.  $K_1 = 71403$ ,  $K_2 = 2586$

АЙУРОВ Р.Н., КАБУЛОВ В.К.

- a) Мен ва университетим
- b) Менинг университетим
- c) Университет ва мен
- d) Сенинг университетинг
- e) To'g'ri javob yo'q

14. «ТАБИАТШУНОСЛИК» so'zini Vijiner usulida shifrlang.  $L=4$ ,  $K=само$

- a) ГБОШПУДБГПКИИК
- b) ПУТЬ\_ГПКИ\_ГБОШ\_СМ
- c) ПУДБ\_ГБОШ\_ГПКЭ\_ЭЛ
- d) ГБОШ\_ПУДБ\_ГПКЭ\_ЭЛ
- e) ЭЛ\_ГБОШ\_ПУДБ\_ГПКЭ

15. С□ЖЕ\_ИДУН\_□АСМ\_ВААЕ\_А□НВ\_А\*НТ Ushbu matnni Gamilton usuli yordamida deshifrlang.

- a) Ватан жуда севаман сени
- b) Жуда севаман сени ватан
- c) Сени жуда севаман ватан
- d) To'g'ri javob yo'q
- e) Gamilton usulida shifrlanmaydi.

*Yuqoridagi testlarga javoblar quyidagi jadvalda keltirilgan:*

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
a	e	b	d	c	a	e	b	d	c	a	e	b	d	c

## ***2. Ma'lumotlarning electron himoyasi***

Umuman olganda, kriptografiyani ikki qismga bo'lish mumkin: ma'lumotlarni berkitishning umumiy usullarini rivojlantirish, shifrlash tizimlarining tahlili va ularning ishonchlilini ta'minlash bilan bog'liq bo'lgan nazariy qism hamda shifrlash tizimlarini ishlab chiqarish va ulardan foydalanish bilan shug'ullanadigan amaliy qismlardan iborat. Ma'lumotlarni himoya qiladigan shifrlar juda ham ishonchli bo'lishi lozim, ya'ni, ular shifrlashni buzishga bo'lgan urinishlarga nisbatan o'ta bardoshli bo'lishi kerak. Shifrnin ishonchliligini asoslash uchun uni ochishga ketadigan ish hajmini chamalash zarur. Bunda agar shifr kalitini topish uchun ketadigan vaqt ma'lumotlarning foydali ravishda ishlatiladigan vaqt intervalidan ko'p bo'lsagina, bunday shifr ishonchi deb hisoblaniladi. Lekin shifrlash bo'yicha yirik olim K.Shennonga ko'ra, shifrlanayotgan informatsiya hajmiga teng bo'lgan uzunlikdagi kalitli shifrgina absolyut ishonchli shifr hisoblanadi. Boshqa barcha shifrlarni ochish mumkin, ammo bunda gap buning uchun kerakli bo'lgan texnik vositalar quvvati va deshifrlash uchun ketadigan vaqtga bog'liq bo'ladi. Jamiyatdagi ma'lumotlar hajmi kam miqdorda bo'lganida unchalik murakkab bo'lmagan shifrlarni ishlatish yetarli bo'lgan. Ma'lumotlar hajminin ko'payib borishi bilan yanada murakkabroq shifrlarni ishlatish zaruriyati paydo bo'lib, ma'lumotlarni shifrovka qilish uchun bu sohaga mahsus o'qitilgan insonlar – ***shifrovkachilar*** jalb qilina boshlandi. Keyinchalik, ma'lumotlar hajmi juda ham ko'payib, rasshifrovkani insonlar bajara olmaydigan xolat yuz bergani tufayli, bu ishni bajara oladigan mexanik va elektorn qurilmalar yaratildi. Komp'yuterlar paydo bo'lganidan

so'ng esa ma'lumotlarni shifrovka va rasshifrovka qilishning yanada zamonaviy va o'ta murakkab usullari paydo bo'ldi va ular turli sohalarda keng miqyosda ishlatilina boshlandi. Kompyuterlar yordamida endi nafaqat ma'lumotlar himoyasi, balki yangi muammolar ham hosil qilina boshlandi, Masalan, electron xujjat almashinishida muhim ahamiyatga ega bo'lgan electron imzo ham ishlatilina boshlandi. Chunki endi electron pochta imkoniyatlari moliyaviy hujjatlarni va konfidentsial ma'lumotlari uzatishda ham ishlatila boshlandi. Elektron tijorat ham ma'lumotlarning konfidentsalligini ta'minlovchi, autentifikatsiya qiluvchu va kirishni boshqaruvchi vositalarni talab qiladi. Raqamli pullar, kriptovalyutalar, **ICO** lar hamda ularning tokenlari va raqamli valyuta almashtirish shahobchalari ham electron himoyaning samarador vositalarini talab qiladi. Xuddi shunday texnik va dasturiy vositalar sifatida ham zamonaviy kriptografik himoya usullardan foydalaniladi. Kriptografiyadan foydalanish quyidagilarni ta'minlab beradi:

- *Konfidentsiallilik* – bu informatsiyaning saqlanishida va uzatilishida ma'lumotlarni ruhsat berilmagan o'qishdan himoya qilishdir. Bu shirflash orqali amalga oshiriladi;
- *Ma'lumotlardan foydalanishning nazorati* – informatsiyadan faqatgina ruxsat berilgan insonlar foydalana olishi kerak;
- *Autentifikatsiya* – ma'lumot uzatuvchi kimliginai aniq bilish imkoniyati. Buni electron raqamli imzo va sertifikat amalga oshirib beradi;
- *Butunlilik* – informatsiyaning saqlanish va uzatilish jarayonida ruxsatsiz o'zgartirila olinmasligi. Bu talab electron raqamli imzo va imitohimoya orqali bajariladi;
- *Informatsiyadan voz kecha olmaslik* – bu ma'lumot uzatuvchining o'zi jo'natgan ma'lumotlardan tonmasligini ta'minlab beradi. Bu ham electron raqamli imzo va sertifikat orqali ta'minlanadi.

Endi electron raqamli imzo hosil qilishda ishlatiladigan bir qancha ommabop algoritmlarni ko'rib chiqamiz. Muloqotdagi ikkala tomon shifrlangan ma'lumotlarni o'zaro almashina olishlari uchun ular ishlatadigan algoritm va kalit (*komp'yuter texnikasi ishlatilganda kalit bu son yoki sonlar ketma-ketligidir*) to'g'risida kelishib olishlari lozim. Shifrlash algoritmlari bir necha yillar davomida yaratiladigan va sozlanadigan matematik funktsiyadir. Ba'zi bir algoritmlar barchaga ma'lum va mashhur bo'lsa, boshqalari mahfiy va konfidentsialdir. Eng taniqli ommabop algoritmlar sifatida **RC4** va **DES (3DES, DESx)** algoritmlarining turli variantlarini ko'satish mumkin. **IDEA** algoritmi esa konfidentsal bo'lib, AQSH xukumati tomonidan ishlab chiqilgan va uning qandayligi hech kimga hech qachon ma'lum qilinmaydi. Yuqoridagi algoritmlarda kalit – ma'lumot almashinish haqida o'zaro kelishayotgan tomonlargagina ma'lum bo'lgan hamda shifrlash algoritmlari tomonidan ishlatiladigan mahfiy son bo'ladi. Shifrlash usullari barcha foydalanilishi uchun mo'ljallangan va konfidentsial turlarga bo'linadi. Foydalanuvchi o'z shart-sharoitlaridan kelib chiqib va qo'yilgan talablarga qarab unisini yoki bunisini o'z faoliyatida ishlatishi mumkin. Shifrlash usullarining esa ikki asosiy turi mavjud: simmetrik kalitli shifrlash va ochiq kalitli shifrlash tizimlari. Bir qancha sabablarga ko'ra, simmetrik kalitli shifrlash usullaridan oldinroq foydalanila boshlandi. Uning amalga oshirilishi uchun ma'lumotlarni shifrlash va deshifrlash maqsadlarida bittagina kalit ishlatiladi. Bu kalitdan ikki shaxs orasida ma'lumot almashinish uchun foydalaniladi. Agarda ma'lumot almashinish jarayonida bir nechta inson ishtirok etsa, u xolda ularning har biri ma'lumot almashinuvchi shaxslar biladigan o'z shaxsiy kalitlariga ega bo'lishlari lozim. Shuning uchun ham bu xolda ma'lumot almashinishda ishtirok etadigan shaxslar soni ortib borishi bilan kalitlar soni ham geometrik progressiya tezligida osha boshlaydi. Bu xolda bir vaqtning o'zida ikki kishi bitta kalitga egalik qilgani uchun u yoki bu xujjatni jo'natuvchi kim ekanligini aniqlashning yoki identifikatsiya qilishning imkoniyati bo'lmaydi. Simmetrik shifrlashning eng ko'p



ishlatiladigan protokoli 1976 yilda AQSH davlati tomonidan kritik bo'lmagan informatsion massivlarini himoya qilish uchun ishlatishga mo'ljallangan kriptografik standart – **RC4** (*Rivest cipher 4*) va **DES** (*Data Encryption Standart*) hisoblanadi.

Shifrlashning chidamliligi foydalaniladigan kalitning ham chidamlilik darajasiga bog'liq bo'ladi. Chidamlilik ikki ko'rsatgich orqali – kalitning uzunligi va uning tasodifiylilik darajasi bilan aniqlanadi. Kalit qanchalik uzun bo'lsa, uning hisoblab toppish ham shuncha murakkab bo'ladi. Lekin ma'lumotlar havfsizligini ta'minlashda asosiysi kalitning chidamliligi ham emas, bunda asosiy muammo – kalitning havfsiz saqlanishidir. Ya'ni kalitni olmoqchi bo'lgan potentsial o'g'ri undan foydalana olmasligi lozim. Mahfiy kalitning himoyasini ta'minlash uchun uni generatsiya qilish, saqlash, almashinish va himoyalashni juda yaxshi amalga oshirish kerak bo'ladi. Havfsizlik tizimlarining ko'pchilik turlarida kalitlar saqlashning apparat modullarida (**HSM** – *Hardware Storage Module*) yoki smart kartalarda saqlanadi. Bu amal mantiqiy/kriptografik himoya bilan bir qatorda unga qo'shimcha ravishda ma'lumot saqlashning fizik darajasini oshirish uchun xizmat qiladi. Simmetrik shifrlash algoritmlarining eng asosiy kamchiligi quyidagidan iborat: ma'lumot almashinishdan avval ma'lumot oluvchiga mahfiy kalitni qandaydir qilib jo'natish kerak. Internet orqali kalitlarni jo'natish juda havfli, shuning uchun kalitni “qo'ldan-qo'lga” disketada yoki oddiy pochta orqali yoki kur'er xizmati vositasida jo'natiladi. Bu ishni bir marta amalga oshirish kifoya, shundan so'ng ma'lumotlarni istalgancha shifrlab jo'natish mumkin. Ammo ekspertlarning fikricha, kalitlarni imkoniyat bo'lsa, tez-tez almashtirib turgan ma'qul. Chunki, agarda kalit biror bir yo'l bilan boshqalar qo'lga tushib qolsa, endi xatlaringiz ochiq, shifrlanmagan xolda ketishi mumkin. Simmetrik algoritm shaxsiy komp'yuteringizdagi fayllarni o'zingiz uchun shifrlashda juda ham qulay. Chunki agarda noutbokingiz yoki planshetingizni biror bir joyda qoldirib ketsangiz yoki o'g'irlatib qo'ysangiz, uning ichidagi ma'lumotlarni shifrlab

qo'yganligingiz tufayli, undagi ma'lumotlarni hech kimsa o'qiy olmaydi. Bunda albatta mahfiy kalitni va kalit kodi yozilgan disketni ham nouytbuk sumkasiga solib qo'ymagan bo'lsangiz, mahfiy ma'lumotlaringizni hech kimsa o'qiy olmaydi. O'z komp'yuteringizdagi ma'lumotlarni shifrlab qo'yishning bir necha xil usullari mavjud bo'lib, ularning ichidan foydalanuvchi uchun bilinmaydigan "*shaffof*" shifrlash dasturlaridan foydalanish tavsiya etiladi. Bunday programmalar komp'uterning mantiqiy diskklarini shifrlash uchun ishlatiladi. Agarda ularni bir martagina komp'yuteringiz uchun sozlab qo'ysangiz, keyinchalik bunday programmalar diskka yoziladigan barcha ma'lumotlarni avtomatik ravishda shifrovka qiladilar va diskdan o'qiladigan ma'lumotlarni ham avtomatik ravishda deshifrovka qilish imkonini yaratadilar. Ya'ni ishlaringizni qulay, tez va havfsiz amalga oshirasiz. Ba'zi vaqtlarda ma'lumotlarni internet orqali simmetrik kodlashtirilib jo'natilishga mo'ljallangan shifrlash algoritmlarini tanlab olish ham maqsadga muvofiq bo'lishi mumkin. Agarda uzatiladigan ma'lumotlar juda ham mahfiy bo'lsa, yuqori darajadagi mahfiylikni ta'minlash uchun ushbu usulni qo'llash mumkin. Bunda yuqori darajadagi mahfiylikka kalitlarning tarmoqli to'plamidan foydalanish orqali erishiladi. Ya'ni, kalitlarning tarmoq to'plami matritsa ko'rinishida bo'ladi. Matritsaning har bir qatori esa shifrlash tizimidagi bittagina foydalanuvchining kalitlari majmui bo'lib xizmat qiladi. Har bir foydalanuchi bir qancha kalitlarga ega bo'lgani sababli, ma'lumotlarni o'g'irlamoqchi bo'lgan shaxs barcha kalitlar to'plamini qo'lga kiritish imkoniyatiga ega bo'la olmaydi.

Shifrlashning ikkinchi usulu ***ochiq kalitlar texnologiyasidan*** foydalanishdir. Bu usulni yana asimmetrik kriptografiya deb ham atashadi. Ushbu usuldan foydalanganda ikkita kalitdan foydalaniladi: ochiq (*ommaviy*) va yopiq (*mahfiy*) kalitlar. Yopiq kalit (*private key*) tasodifiy ravishda tanlangan tasodifiy son sifatida bo'lishi yoki kompyuterdagi tasodifiy sonlar datchididan tanlab olinishi kerak. Ochiq kalit esa (*public key*) yopiq kalit

orqali hisoblanib topilishi lozim. Ammo bunda teskari ish amalga oshirishining umuman ilojisi bo'lmazligi kerak. Ochiq kalit faqatgina ma'lumotlarni shifrlash uchun ishlatilishi kerak, yopiq kalit esa ma'lumotlarni ma'lumotlarni deshifrlash uchun ishlatiladi. Ushbu usulning afzallik tomonlari nimada? Bu usulda kalitlarni almashinish jarayoni soddalashadi – aloqa kanali bo'yicha faqatgina ochiq kalit jo'natiladi, mahfiy kalit esa uning egasida bir nusxadagina saqlanadi. Uni bilmasdan turib, ochiq kalit yordamida ma'lumotlarni rasshifrovka qilish umuman mumkin emas. 1978 yilda yaratilgan asimmetrik shifrlash algoritmi **RSA** (*Random Signature Algorithm*) boshqa sohalar bilan bir qatorda elektron hujjatlarda va elektron raqamli imzoda keng miqyosda ishlatilina boshlandi. **RSA** ning diqqatga sazovor tomonlaridan biri shundaki, unda asimmetrik shifrlash va elektron raqamli imzo hosil qilish uchun bir xildagi amallar bajariladi. Bu tizim vaqt imtihonidan muvaffaqiyatli o'tdi va xozirgi davrda ishlab chiqarishdagi kriptografiyaning de-facto standartiga aylandi. Bir qancha xalqaro tashkilotlar ham **RSA** ni rasmiy standart sifatida tan olganlar. **RSA** kriptotizimida mahfiy kalit elektron raqamli imzoni hisoblash uchun yoki ma'lumotlarni rasshifrovka qilish uchun ishlatiladi. Ochiq kalit esa elektron raqamli imzoni tekshirish va ma'lumotlarni shifrovka qilish uchun ishlatiladi.

**DSA** algoritmi - (*Digital Signature Algorithm*) 1981 yilda yaratilgan bo'lib, elektron raqamli imzo uchun AQSH standarti (*Digital Signature Standart* – **DSS**) sifatida ishlatiladi. **DSS** standartining aniqlanuviga ko'ra, **DSA** algoritmi xesh-funktsiya sifatida **SHA** algoritmini ishlatishni ko'zda tutadi. Bu algoritmning ko'rsatgichlari mahfiylashtirilmagan, **DSA** algoritmi AQSH da ham raqamli imzoning standarti sifatida ishlatiladi. U faqatgina elektron raqamli imzoni xosil qilish uchungina ishlatilib, ma'lumotlarni shifrlash uchun ishlatilmaydi.

Kalitdan foydalangan xoldagi istalgan shifrlash algoritmini kalitlarning barcha qiymatlarini tanlash usuli orqali rasshifrovka qilish mumkin. Ammo bunda rasshifrovka qilish uchun zarur bo'lgan komp'yuter quvvati kalit

uzunligi oshishi bilan eksponentsial ravishda ko'payadi. Kriptografik tizimning ishonchliligi uning eng kuchsiz qismi xususiyati bilan aniqlanadi. Shuning uchun shifrlash tizimining har bir qismini – algoritmini, shifrlashni qo'llash usulini va kalitlardan foydalanish siyosatini ishlab chiqishda juda hushyor bo'lish talab etiladi.

### ***3. Elektron imzo va xesh-funktsiyalar***

Electron raqamli imzoni hosil qilish, uni tekshirish, raqamli valyutalar bilan ishlash kabi bir qancha kriptografik operatsiyalar (*o'zgartirishlar*) chegaralangan ma'lumotlar ustida bajariladi. Shuning uchu ham katta hajmdagi (*masalan, 125 megabaytli ma'lumot*) fayllarga electron raqamli imzo qo'yishdan avval undan xesh-funktsiya hisoblanadi va shundan so'ng uning qiymatiga electron raqamli imzoni hisoblaydilar. Undan tashqari, parollarni ham ma'lumotlar bazasida ochiq xolda emas, balki xeshlangan xolda saqlash maqsadga muvofiqdir. Shunday qilib **Xesh** – istalgan uzunlikdagi ma'lumotlar massividan oldindan aniqlangan uzunlikdagi qandaydir qiymat olish uchun amalga oshiriladigan o'zgartirishdir. Xesh-funktsiyani tushunish uchun eng oddiy misol nazorat yig'indilarini hisoblashdir (*kontrol'nie summi*). Xeshlashning dasturiy va kriptografik turlari mavjud. Kriptografik xesh dasturiy xeshdan ikki xossasi bilan farqlanadi: orqaga qaytmaslik va kolliziyalardan ozodligi. Kalitsiz xesh funktsiyalar ikki guruhga bo'linadilar: kuchli xesh-funktsiyalar va kuchsiz xesh-funktsiyalar. Kuchsiz xesh funktsiya deb, quyidagi shartlarni bajaruvchi bir tomonlama **H(x)** funktsiyaga aytiladi:

- 1) **X** argument istalgan uzunlikdagi bitlar qatori bo'lishi mumkin;
- 2) **H(x)** funktsiyaning qiymati aniq uzunlikka ega bo'lgan bitlar qatori bo'lishi lozim;
- 3) **H(x)** funktsiyaning qiymatini hisoblash oson bo'lishi kerak;

4) Har qanday aniq  $\mathbf{x}$  uchun hisob-kitoblar vositasida  $\mathbf{H}(\mathbf{x}^*) = \mathbf{H}(\mathbf{x})$  bo'ladigan  $\mathbf{x}^*! = \mathbf{x}$  qiymatini topish mumkin bo'lmasin.  $\mathbf{H}(\mathbf{x}^*) = \mathbf{H}(\mathbf{x})$  xolatidagi  $\mathbf{x}^*! = \mathbf{x}$  juftligi xesh-funktsiyaning kolliziyasi deb ataladi.

Kuchli xesh-funktsuya deb kuchsiz funktsiya uchun yuqoridagi 1-3 shartlarni va quyidagi 5-shartni bajaradigan bir tomonlama  $\mathbf{H}(\mathbf{x})$  funktsiyaga aytiladi:

5)  $\mathbf{H}(\mathbf{x}^*) = \mathbf{H}(\mathbf{x})$  bo'ladigan har qanday  $\mathbf{x}^*! = \mathbf{x}$  qiymatini hech qanday hisob-kitoblar yordamida topish mumkin bo'lmaydi.

Har qanday simvollar ketma-ketligi kabi, elektron raqamli imzoni hisoblashning formulasini matematik ko'rinishda quyidagicha tasvirlash mumkin:

$$\mathbf{S} = \mathbf{F}(\mathbf{h}(\mathbf{M}), \mathbf{Ks})$$

Bu yerda  $\mathbf{M}$  – ma'lumot matni,  $\mathbf{Ks}$  – mahfiy kalit,  $\mathbf{h}(\mathbf{M})$  – xeshlashtirish funktsiyasi.

Yuqorida keltirilgan ifodaga ko'ra, elektron raqamli imzoni xosil qilish uchun boshlang'ich xomashyo sifatida ma'lumotning o'zi emas, balki uning xeshi olinadi (*ya'ni, ma'lumotning xesh-funktsiya yordamida xosil bo'lgan natijasidan foydalaniladi*). Chunki imzo bilan tasdiqlanuvchi matn kattaligi noldan to bir necha megabaytgacha bo'lishi mumkin. Ayniqsa mu matn grafik elementlarga ega bo'lsa, yanada kattalashib ketishi mumkin. Ammo amaliyotda qo'llaniladigan barcha xeshlashtirish algoritmlari hisob-kitoblar uchun matnning oldindan belgilangan standart uzunlikda bo'lishini talab qiladi. Masalan, Rossiyada ishlatiladigan **ЭЦП ГОСТ Р 34.10-94** algoritmidan bu standart uzunlik 32 baytga teng bo'lishi talab qilinadi. Demak, xesh-funktsiya algoritmining hal qilishi kerak bo'lgan asosiy masala - istalgan uzunlikdagi va hajmdagi ma'lumotdan kerakli uzunlikdagi (*masalan, 32 baytli*) sonlar ketma-ketligini hosil qilishdir.

Bunday talablarga javob beradigan xesh-funktsiya algoritmini yaratish unchalik qiyin ish emas, ammo bu funktsiya bir qancha talablarga javob berishi kerak. Eng avvalo, xesh-funktsiya yordamida olingan natija

boshlang'ich ma'lumotga birga-bir mos kelsin va bu natija boshlangi'ch ma'lumotning har qanday o'zgarishida ham unga yana birga-bir mos kelsin. Undan tashqari, xesh-funktsiya shunday hisoblanilishi kerakki, har qanday **M** ma'lumot uchun  $h(M) = h(M^*)$  bo'lgan **M\*** ma'lumotni tanlab olish yoki topish mumkin bo'lmasin. Boshqacha so'zlar bilan aytganda,  $h(M) = h(M^*)$  shartni qanoatlantiruvchi **M** ma'lumot va uning xesh-funktsiyasi ma'lum bo'lganida, **M\*** ma'lumotni muvaffaqiyatli hisoblashga ketadigan mehnat sarfi ma'lumotlarni to'g'ridan-to'g'ri saralash uchun zarur bo'lgan mehnat sarfiga ekvivalent bo'lishi kerak. Bu shartning bajarilmasligi potentsial firibgarga imzoni o'zgartimasdan turib, ma'lumotlarni almashtirib qo'yish imkoniyatini yaratishi mumkin. Boshqa tomondan qaraganda, ko'pchilik ma'lumotlar uchun xesh-funktsiyalar bir xil bo'lishi mumkin, chunki mumkin bo'lgan ma'lumotlar to'plami xesh-funktsiyalarning mumkin bo'lgan to'plami sonidan ancha ko'p miqdorda bo'ladi. Ya'ni, ma'lumotlar soni cheksiz miqdorda bo'lib, xesh-funktsiyalar soni esa  $2^N$  ga teng bo'ladi, bu yerda **N** – xesh funktsiyaning bitlardagi uzunligi.

Xozirgi paytda eng keng tarqalgan xesh-funktsiyalar algoritmlari sifatida quyidagilarni ko'rsatishimiz mumkin:

- Rossiyada qo'llaniladigan standart **ГОСТ 3 34.11-94** xesh-kattalikni 32 bayt kattalikda hisoblaydi.
- **MDx (Message Digest)** – chet mamlakatlarda eng ko'p tarqalgan xeshlashtirish algoritmlari oilasi. Masalan, **MD5 Microsoft Windows** ning oxirgi versiyalarida foydalanuvchi parolini 16 baytli songa aylantirishdan foydalaniladi.
- **SHA-1 (Secure Hash Algorithm)** – kirish ma'lumotlarini 20 baytli xesh-miqdorga aylantirishning hisoblash algoritmi. Bu algoritmi ham jahon miqyosida keng tarqalgan bo'lib, ko'pincha ma'lumotlarni himoyalashning tarmoq protokollarida ishlatiladi.

Xesh-funktsiyalar elektron raqamli imzo hosil qilishdan tashqari, hisoblash tizimlarida foydalanuvchilarni autentifikatsiya qilish uchun ham

AYULOV R.H., KADULOV V.R.

ishlatiladi. Xesh-funktsiyalardan foydalanishga asoslangan bir qancha kriptografik autentifikatsiya protokollari ham ko'pchilikni tashkil qiladi.

Kalitlar juftligidan foydalanish ham juda qiziqarli va foydali hisoblanadi. Siz ikkita kalitga – ochiq va yopiq kalitga egasiz deb faraz qilamiz. Sizning maqsadingiz – barcha ma'lumotlar siz uchun shifrlangan xolda kelsin. Buning sababi, masalan, sizning hamkasabalarangiz sizning mijozlaringizni tortib olmasligiga yo'l qo'maslikdir. Endi o'zingizning barcha respondentlaringizga ma'lumotlarni sizga shifrlangan xolda jo'natishlari uchun ochiq kalitingizni tarqatasiz (*bu kalitni saytingizga ham qo'yishingiz mumkin*). Shifrlangan ma'lumot olganingizdan so'ng, yopiq kalit yordamida uni bimalol o'qib olasiz. Ammo bu ma'lumotni olgan har qahday inson sizning ochiq kalitingiz yordamida bu ma'lumotni o'qiy olmaydi. Yopiq kalit esa unda yo'q. Yopiq kalit faqatgina uning egasida bo'lgani tufayli, ushbu usulning paydo bo'lishi kriptografiya usulining ishlatilish chegaralarini yanada kengaytirish imkonini yaratdi. Endi elektron raqamli imzo yaratish orqali autentifikatsiya muammosini hal qilish uchun, electron pullar bilan havfsiz ishlash uchun, himoyalangan ovoz berish tizimlarini yaratish uchun, electron xujjatlarni notarial tasdiqlash uchun va turli xildagi kriptoalyutalar tizimini yaratish uchun ushbu usulni bimalol qo'llash mumkin bo'ldi. Endilikda foydalanuvchi bir-biri bilan bog'liq bo'lgan ikkita kalitni – ya'ni, kalitlar juftligini generatsiya qilishi mumkin bo'ldi. Ochiq kalit mahfiy bo'lmagan kanallar orqali foydalanuvchi ma'lumot almashinishni istagan insonlarga jo'natiladi. Foydalanuvchining ochiq kalitini bilgan xolda unga yo'naltirilgan ma'lumotlarni shifrlash mumkin bo'ladi, ammo uni rasshifrovka qilish uchun esa kalitlar juftligining ikkinchisi kerak bo'ladi. Bunda ochiq kalit yopiq kalitni aniqlash uchun hech qanday imkoniyat bermaydi. Nazariy jihatdan bu masalani yechish mumkin – lekin bu ish juda katta miqdordagi hisoblash ishlari hajmini bajarishni talab qiladi. Ma'lumotni rasshifrovka qilish vaqti juda katta (*bir necha oylar va yillar*)

bo'lgani uchun, uni rasshifrovka qilingan taqdirda ham, u vaqtga kelib ma'lumot o'zining aktualligini yo'qotadi va u endi hech kimga kerak bo'lmay qoladi.

Agar siz biror bir tanishingiz bilan ma'lumotlarni himoyalangan xolda electron imzo vositasida almashinishni istasangiz u xolda quyidagi amallarni bajarishingiz lozim bo'ladi:

- ✓ Eng avvalo electron imzolar kalitlarini yarating – har biringiz o'z ochiq va yopiq kalitga ega bo'lishingiz kerak;
- ✓ Yopiq kalitlarni o'zingizda olib qoling va ochiq kalitlarni o'zaro almashining;
- ✓ Yopiq kalit bilan tanishingizga jo'natilayotgan xatga electron imzo qo'ying va xatni electron imzo bilan birgalikda do'stingizga jo'nating;
- ✓ Elektron imzo bilan ta'minlangan ma'lumotni olgandan so'ng, do'stingiz sizning ochiq kalitingiz yordamida bu xatning xaqiqiyligini tekshiradi;
- ✓ Tekshirish natijasi ikki javobdan biri – to'g'ro yoki noto'g'ri bo'ladi;
- ✓ Shunday qilib, elektron imzo ma'lumotning haqiqiyligini aniqlab beradi;
- ✓ Agarda ma'lumot uzatish jarayonida unda biror bir o'zgartirishlar kiritilgan bo'lsa, bu ish darxol ma'lum bo'ladi;
- ✓ Elektron imzoning yana bir muhim jihati – ma'lumot muallifining tasdiqlanishidir. Ko'pincha elektorn raqamli imzo fayliga kalit bilan birga uning egasi ismi-sharifi, ish joyi, electron imzoning amal qilish muddati kabilar ham yozib qo'yiladi. Ma'lumot yoki xujjat ostidagi imzoga esa mahfiy kalitdagi ma'lumotlar nushalanadi – bu esa o'z navbatida mualliflikni aniqlashga imkon beradi. Demak, ochiq kalitni kim jo'natgani haqidagi ma'lumotlarni yodda saqlash talab qilinmaydi. Bu juda ham muhim, chunki sizda bir qancha insonlarning ochiq kalitlari bo'lishi mumkin.



Ammo yopiq kalitni juda ham mahfiy ravishda saqlashingiz talab etiladi – chuni biror bir kimsa uni bilib qolsa, u sizning electron imzoingizni qalbakilashtirib, xujjatlarga imzo qo'yishi mumkin. Agarda kalitingizni yo'qotib qo'ysangiz, albatta zudlik bilan kerakli bo'lgan chora-tadbirlarni ko'ring. Va eng avvalo, bu ma'lumotni o'z potentsiyal adresatlaringizga tezda yetkazing – *“mening ilgarigi electron imzoimni endilikda, bugun . . . . . dan boshlab noto'g'ri deb hisoblang”*. Agar bu isni o'z vaqtida qilmasangiz, hozirgina bir qancha bo'sh qog'ozlarga imzo chekdim, istalgan inson unga istalgan ma'lumotni yozib, boshqalarga jo'natishi mumkin deyishingiz mumkin.

Ochiq kalitli shifrlash tizimning yuqorida ko'rsatilgan biq qancha afzalliklariga qaramasdan, uning bir qancha kamchiliklari ham mavjud. Bular ichida eng asosiysi – bu usul simmetrik kalitli tizimga qaraganda anchagina sekin ishlaydi. Huddi shuning uchun ham kundalik hayotda kombinatsion usuldan foydalaniladi. Bunda ma'lumotlarni shifrlash uchun simmetrik (*seansli*) kalitlar ishlatilib, ular o'z navbatida tarmoq orqali seans kalitlarini jo'natishda ochiq kalitlardan foydalangan xolda shifrlanadi. Buning uchun quyidagi amallarni bajarish talab etiladi:

- Bir-biriga ma'lumot jo'natmoqchi bo'lgan ikki inson ikki juft kalit tayyorlaydi: asimmetrik shifrlash uchun mo'ljallangan ochiq va mahfiy kalit hamda electron raqamli imzoning ochiq va mahfiy kalitini;
- Bu ikki inson ochiq kalitlar bilan o'zaro almashinadilar va ulardan biri ikkinchisiga o'z mahfiy kaliti orqali imzolangan ma'lumotni jo'natadi;
- Keyin birinchi inson simmetrik shifrlashning kaliti **K** ni tasodifiy ravishda generatsiya qiladi va shu shifr bilan jo'natilayotgan xatni shifrlaydi;
- Shundan so'ng, olinadigan ma'lumotni rasshifrovka qilish mumkin bo'lishi uchun **K** kalitni o'z do'stining asimmetrik shifrlash ochiq

kalitida shifrlaydi (*simmetrik shifrlashning kalitini ochiq ko'rinishda jo'natish mumkin emas*) va uni shifrlangan hatga qo'shib qo'yadi;

- Ikkinchi inson shifrlangan ma'lumotni olganidan so'ng, o'z asimmetrik mahfiy ochiq kaliti yordamida **K** kalitni rasshifrovka qiladi va uning yordamida xatni ham rasshifrovka qiladi;
- Keyin esa u do'stining xatidagi elektron raqamli imzosi ochiq kaliti yordamida bu xat o'z do'stidan o'zgarmagan xolda kelganiga ishonch hosil qiladi.

Ochiq va yopiq kalitlarning o'zaro mos kelishini tekshirish uchun ularni qo'shimcha ravishda himoya qilish va identifikatsiya qilish talab etiladi. Bu maqsadni amalga oshirish uchun yana bir hujjat – elektron sertifikat talab etiladi. Elektron sertifikat ochiq kalitni uning konkret egasi yoki qandaydir amaliy dastur bilan bog'lab turadi. Sertifikatning o'zi ham tasdiqlangan bo'lishi kerak, bu bilan uning haqiqiyligi tasdiqlanadi. Ushbu tasdiqlashni sertifikatga o'z elektron imzosini qo'ygan sertifikatlash markazi amalga oshiradi. Sertifikatlashtirish markazi elektron raqamli imzo tizimining markaziy elementi bo'lib hisoblanadi. Sertifikatlash markazining ochiq kalitini ishlatgan xolda istalgan foydalanuvchi markaz tomonidan chiqarilgan sertifikatning haqiqiyligini tekshirib ko'rishi mumkin. Tekshirish jarayoni shunday iboratki, unda sertifikat egasining nomi bilan ochiq kalitning mos kelishi tekshiriladi.

Ochiq kalitlar infratuzilmasi kriptografiya asosida himoyalangan tarmoq ulanishlarini tashkil qilishda (*masalan, S/MIME, SSL, IPSEC*) turli xil amaliy ilovalarda (*masalan, elektron pochta, web-ilovalar, elektron tijorat*) yoki elektron xujjatlar elektron raqamli imzolarini xosil qilishda ishlatiladi. Har qanday ochiq kalitli kriptografik algoritmlar kabi elektron raqamli imzoning Internet muhitida ishlatilishi juda ham qulay – siz o'z ochiq kalitingizni imzo qo'yilgan ma'lumotni kerakli insonga jo'natishingizdan avval istalgan adresatga jo'natishingiz yoki ochiq kalitni Internetdagi biror bir resursga

joylashtirib qo'yishingiz mumkin. Lekin bunda havfsizlik darajasi biroz pasayadi, chunki ochiq kalitlar almashtirilib qo'yilishi mumkin. Ammo, ochiq kalitlarni almashtirib qo'yishga qarshi kurash usuli mavjud – bu ularning sertifikatlashtirishini amalga oshirishdir.

Endi ochiq kalitlarning infratuzilmasi (*Public Key Infrastructure - PKI*) haqida batafsilroq to'xtalib o'tamiz. Ushbu tushuncha o'tgan asrning yetmishinchi yillarida Halqaro elektr aloqalar ittifoqi (**ITU**) tomonidan **X500** standartlar seriyasiga mansub tadbir sifatida ishlab chiqarilgan. Bu standartlar foydalanuvchilar haqidagi ma'lumotlar mavjud bo'lgan ma'lumot bazalari tuzilishi qanday bo'lishini aniqlab bergan. Ochiq kalitlarning infratuzilmasi ma'lumotnomasi **PKI** dan foydalanuvchilar ma'lumot olishlari mumkin bo'lishi kerak va u eng yangi ma'lumotlarni va ma'lumotlarning haqiqiylik muddatini o'z ichiga olishi lozim, o'chirilgan informatsiya haqida esa ma'lumotlar ham bo'lishi zarur. **PKI** ma'lumotnomalari mahfiy yozishmalarni va savdo operatsiyalarni amalga oshirishda ishlatilgani uchun, undagi ma'lumotlarning sifati va aniqligi katta ahamiyatga ega bo'ladi. Ochiq kalitlarning infratuzilmasi ma'lumotnomasi **PKI** dagi ma'lumotlarning eskirib qolishiga yo'l qo'yish mumkin emas, chunki bu xolda ma'lumotnomaga ishonch yo'qoladi va tabiiyki, endi unga bo'lgan talab ham yo'qoladi. Ammo **PKI** faqatgina ma'lumotnoma emas, uning tarkibiga kalitlar bilan ishlashni amalga oshirib beruvchi dasturiy-texnik vositalar va tashkiliy-texnik tadbirlar ham kiradi. Bunday tizimni yaratishdan asosiy maqsad - kalitning ochiq qismini uning yopiq qismi bilan birgalikda qo'shimcha himoyasini va identifikatsiyasini ta'minlashdir. Bu funktsiyani sertifikatlashtirish markazining elektron raqamli imzosi bilan tasdiqlangan sertifikatlar amalga oshirib beradilar. Ochiq kalitlar infratuzilmasi tarkibiga ***sertifikatsiya markazi, registratsiya markazi va tarmoq ma'lumotnomasi*** kiradi. Har bir xizmat o'zining nomi bilan bog'liq bo'lgan funktsiyalarni bajaradi. Ushbu xizmatlarga kirish uchun turli xildagi tarmoq protokollari ishlatiladi. Infratuzilmaga kalitlar saqlaydigan va mijoz dasturlariga ega

bo'lgan foydalanuvchilarni ham kiritish mumkin. Sertifikat o'z foydalanuvchisi va uni bergan organ haqidagi ma'lumotlarga ega bo'ladi. Bunday ma'lumot o'z tarkibiga quyidagilarni oladi:

- Ochiq kalit va u ishlatadigan algoritm;
- Foydalanuvchiga tegishli fakul'tativ atributlar;
- Sertifikatni tasdiqlovchi markazning raqamli imzosi;
- Sertifikatsiya markazining manzili;
- Sertifikatning amal qilish muddati;
- Sertifikatsiya markazining sertifikat olishdan ilgari sifat ko'rsatgichi

Shunday qilib, sertifikat bergan markaz sub'ektning ochiq kaliti va uni identifikatsiya qiladigan ma'lumotlarning xaqiqiyligini tasdiqlab beradi.

Qonunga muvofiq sertifikatsiya funktsiyasi elektron raqamli imzolar kalitlari registratsiyasi markaziga yuklatilgan. O'zbekiston Respublikasining 2013 yil 11 dekabrda "Elektron raqamli imzo haqida" gi Qonuniga muvofiq: *"**elektron raqamli imzo** – elektron raqamli imzo kalitidan foydalangan xolda elektron hujjatdagi ma'lumotlarni mahsus qayta ishlash natijasida hosil qilingan elektron hujjatdagi imzo bo'lib, elektron raqamli imzoning ochiq kaliti vositasida elektron hujjatda o'zgarishlar yo'qligini tekshirishga va elektron raqamli imzoning egasi yopiq kalitini identifikatsiya qilishga imkon beradi"*. Elektron raqamli imzolarni registratsiya qilish markazi **RSA Keon** dasturiy-texnik kompleksidan foydalanadi. Ushbu dasturiy-texnik kompleks elektron raqamli imzo infratuzilmasi tarkibiy qismlarining barcha elementlarini o'z tarkibiga oladi va tashkilotlarni boshqarish bo'yicha boshqa tizimlar bilan birgalikda ishlay oladi.

#### ***4. Kriptovalyutalarning tarixi***

Internet va elektron savdo rivojlangan sayin insonlarning “*uzoqlardan-masofadan turib*” elektron pullar to’lashlariga to’g’ri kela boshladi. Bunda pulni masofadan turib qo’ldan qo’lga berishning esa umuman iloji yo’q. Shuning uchun ham pullarni bir insondan ikkinchisiga masofadan turib o’tkazish jarayonida o’ziga hos vositachilarga, ya’ni elektron to’lov tizimlari, bank yoki kur’yerlarga murojaat etish kerak bo’ladi. Har qanday vositachi esa bajarayotgan pul o’tkazmalariga bog’liq bo’lgan operatsiyasi uchun qandaydir to’lov olib qoladi, chunki hech kim tekinga ishlashni hohlamaydi. O’tkazilayotgan pul miqdori qancha ko’p bo’lsa, vositachiga bo’lgan to’lovlar tufayli pulni yo’qotish ham shunchalik ko’p bo’ladi, albatta. Axborot texnologiyalari va elektron savdo rivojlangani sari ko’pchilik odamlar pul o’tkazmalari bilan bog’liq harajatlarni kamaytirish borasida o’ylanib qolishdi, ya’ni, qanday qilib ushbu xarajatlarni kamaytirish va pul o’tkazmalari foydali ish koeffitsientini iloji boricha yuz foizga oshirgan xolda elektron biznesni yuritish mumkin?



Bu borada turli xildagi taklif va molohazalar juda ko'p edi, lekin ularning barchasi bir qancha sabablarga ko'ra rad etildi. Chunki tovar va hizmatlar oldi-sottilaridagi vositachilarga bo'lgan to'lovlarni olib tashlaganda ham, turli-tuman firibgarlardan qanday himoyalanish – pulni aynan Siz o'tkazganingiz yoki uni olganingizni qanday isbotlash mumkin? Bu muammoning yechimi 2009-yillarda Satoshi Nikamoto deb nomlangan shaxs yoki shahslar guruhi tomonidan murakkab kriptografik matematik xisob-kitoblar natijasida ishlaydigan yangi elektron to'lov tizimini ommaga taqdim etgandan so'ng topildi. Bunday to'lovlarni amalga oshirishda ishlatiladigan pul birligining nomi esa **bitkoin** deb ataldi. Bitkoin kriptografik elektron pul birliklari maxsus elektron hamyonlarda saqlanib, bunday hamyonlarga pul tushirish va ularni turli xil maqsadlarda ishlatish mumkin.



Biror-bir bitcoin-hamyon hisobidan qancha elektron pul ketgani yoki unga kelganini aniqlash uchun, mutaxassislar bir hamyondan yoki boshqa manzildan ushbu elektron hamyonga qancha bitkoinlar kelganini barchaga ochiq xolda ko'rsatishni taklif etdilar. Ya'ni, siz kriptovalyuta tarmog'iga ulanganingizda, barcha bitcoinlar oldi-sotdisini aniq va ravshan ko'rishingiz va kuzatishingiz mumkin bo'ladi. Shuningdek, barcha bitkoin hamyonlar anonimdir (ya'ni, *hamyonning egasi kim ekanligi aytilmaydi*), shuning uchun ham Sizning tanishingiz qaysi hamyon uniki ekanini aytmagan bo'lsa, Siz hech qachon bu haqida bila olmaysiz. Tizimdagi hisob-kitoblarni muntazam ravishda amalga oshirib borish kerakligi tufayli, bitcoinlarning ma'lumotlar bazasi tezkor ishlashi uchun katta quvvatli zamonaviy kompyuterlar kerak bo'ladi. Bunday quvvatli komp'yuterga ega bo'lish uchun minglab kompyuterlarni yagona tarmoqqa ulash talab etiladi. Bu kompyuterlar foydalanuvchilarning komp'yuterlari ham bo'lishi mumkin albatta. Ulardan biri esa istagingizga ko'ra Sizning komp'yuteringiz bo'lishi ham mumkin. Agarda foydalanuvchi, o'z kompyuteri videokartasi quvvatini tegishli dasturlardan foydalangan xolda bitcoin tizimini qo'llab-quvvatlash uchun taqdim etsa, bu yordami uchun unga o'sha bitcoin valyutasining o'zida mukofot berishadi. Bunday pul topish usuli esa **“mayning”** deya nom olgan.



Quyida zamonaviy kriptovalyutaning afzallik va kamchiliklar tomonlarini keltirib, ularga izoh beramiz.

- ***Chegaralangan***. Kriptovalyuta yaratilgan algoritmgaga asosan, ja'mi 21 000 000 gacha bitcoin topish mumkin, bundan so'ng esa bitkoin yetishtirish to'xtatiladi. Buning oqibatida nima bo'lishini hech kim bilmaydi, agarda moliyaviy portlash bo'lmasa, kriptovalyuta muomalada qoladi va vaqti-vaqti bilan o'z kursini o'zgaritirib turaveradi.
- ***To'liq mahfiylik***. Bitcoin-hamyonning raqamlari orqali uning egasi kim ekanligini bilib bo'lmaydi, buning oqibatida noqonuniy pul aylantirish va firibgarlikka yo'l ochiladi.
- ***Ta'minlanmaganlik***. Kriptovalyuta, real pullarga o'xshab, doimiy rezerv bilan ta'minlanmagani va bu bilan bog'liq boshqa sabablarga ko'ra, bitcoin kursi kutilmaganda to'liq nolga tushib ketishi ham hech gap emas.
- ***Rasmiy ravishda ishlamaydi***. Bitcoin moliya tizimiga yomon ta'sir ko'rsatishi mumkin, shu sababli ko'p davlatlar (*shu jumladan, bizning mamlakat ham*) kriptovalyutaga ishonchsizlik bilan qaraydi. Rossiyada bitcoin yetishtirish bilan shug'ullanganlarni javobgarlikka tortish bo'yicha qonun tayyorlashgan, lekin hozircha bu ish to'liq yo'lga



qo'yilmagan. Balki bitcoinlar hech qachon rasmiy ishlamasa ham kerak, chunki uni qonuniylashtirishsa, bitkoin real valyutani o'rnini egallashi ham mumkin bo'ladi.

- **Unchalik mashxur emas.** Hozircha ko'pgina moliyaviy muassasalar, Internet-do'konlar va boshqa servislar bitcoinga ishonishmaydi va kriptovalyuta evaziga maxsulot sotmaydilar. Mashxurlashishi chegaralangani boyis Bitkoin to'liq ishlatilmayapti.



Hozirgi davrdagi eng mashhur kriptovalyutalarning emblemalarini (*shartli belgilari, piktogrammalarini*) quyida nazardan kechirishingiz mumkin:



Kriptovalyutalarni mayining qilish uchun foydalanish mumkin bo'lgan eng yaxshi dasturiy ta'minotlarga quyidagilarni kiritishimiz mumkin:

**CGMiner** – Ushbu dastur virtual pullarni topish bo'yicha ishlaydigan professionallar uchun mo'ljallangan. Ammo uning to'liq quvvat bilan ishlashi uchun faqatgina katta quvvatli komp'yuterlar talab qilinadi. Foydalanuvchiga esa MS DOS buyruqlarini yaxshilab o'zlashtirib olish zarur bo'ladi. Dasturning ijobiy tomonlariga videokarta ishini tezlashtirish funktsiyasi mavjudligi va buning natijasida xeshlashtirish jarayoni tezlashtirilishini kiritish mumkin. Bundan tashqari, dasturning optimal ishlash rejimini tanlash imkoniyati ham uni boshqa dasturlardan farq qiladi.

**Diablo Miner** – Hozirgi vaqtda mavjud bo'lgan barcha operatsion tizimlarda bir xilda ishlay oladigan va kriptovalyutalarni mayning qilishga mo'ljallangan saytdir.

**Ufasoft Miner** – Ushbu dastur ishchi ko'rsatgichlarini sozlash mumkinligi tufayli mutaxassislar orasida ancha ommabop hisoblanadi. Har bir foydalanuvchi, o'z istak-xoxishiga ko'ra, video karta bo'yicha, yadrolar soni bo'yicha, oqimlar bo'yicha va pu'llar manzillari bo'yicha o'zgartirishlar kiritishi mumkin.

**BFG Miner** – Bu dasturda esa foydalanuvchilar qo'l rejimida pullarni sozlashi va ventilyatornong tezligini boshqarishi mumkin.

**Phoenix** – Ushbu dastur juda samarador ishlaydiganlar qatoriga kiradi va ish unumdorligini 20% ga ko'tarish imkonini beradi. Dasturni yuklash uchun kriptovalyuta mayningiga mutaxassislashgan saytlarining biriga kirish yoki shunday tematik forumlarga kirish talab etiladi.

**Solo-mayning jarayoni** virtual pullarni mustaqil ravishda topishini anglatadi. Ammo, yuqorida ko'rsatib o'tilganidek, bu ish xozirgi davrda ancha murakkab bo'lib qoldi va uni yo'lga qo'yish uchun professoionalizm hamda yaxshigina investitsiya talab etiladi. Albatta ko'pchilik insonlar bunday miqdorda pul mablag'lariga ega emas, shuning uchun ham maynerlar “**pu'l**” deb atalmish guruhlarga birlashib ish yuritadilar.

**Pu'l-mayning** – bir qancha kichik maynerlar o'zlarining resurslarini bir joyga yiqqan xolda kriptovalyuta mayningi bilan shug'ullanadilar. Bu yakka xolda ishlagandan ko'ra ancha havfsizroq faoliyat turi hisoblanadi. Pu'l ni tanlash uchun tematik forumlarga o'tish va u yerdan xamkorlarni topish mumkin. Pu'lni tanlashda quyidagilarga ahamiyat berish kerak bo'ladi:

- *Foydalanuvchilarning ko'proq bo'lishi;*
- *Umumiy hisoblash quvvati yetarli bo'lishi;*
- *On-line resursning komission to'lovi kattaligi qandayligi.*

**RDP-mayning** – Bulutli deb nomlangan texnologiyalarning keng miqyosda ishlatilishi kriptovalyutalar topishning RDP-mayning kabi kollektivizmga asoslangan turlari paydo bo'lishiga olib keldi. Uning quyidagi ijobiy tomonlari mavjud:

- *Juda qimmat turadigan mayner qurilmalarini sotib olishning shart emasligi;*
- *Hisoblash quvvatlarini arzonga ijaraga olish yoki ularni doimiy ishlatish uchun qo'lga kiritish;*
- *Mayninglik faoliyatini kam mablag' sarf qilgan xolda amalga oshirish;*
- *Kriptovalyutalarning RDP-mayning usuli kapital qo'yilmalarni asta-sekin ko'paytirishni ko'zda tutadi. Pullarni bosqichma-bosqich ko'paytirish yoki olingan dividendlarni reinvestitsiya qilish ham mumkin.*

Mayningning bulutli platformalarida boshlag'ich bonusni tekinga olish imkoniyati ham bor. Ushu bonus katta emas, ammo ishni boshlash uchun yetadi. Bu xolat esa reklama ro'lini o'ynab, mayning jarayoniga yangi kriptovalyutachilarni jalb qilishga yordam beradi. RDP-mayningda birlamchi bonusning miqdori bir ming dogikoin atrofida bo'ladi. Foydalanuvchi mayning faoliyatini boshlash uchun akkauntni faollashtirishi va bonusni hisoblash quvvatiga almashtirishi kerak. Shundan so'ng esa virtual pullarni ishlash jarayonini boshlash mumkin bo'ladi. Hisoblash quvvatining minimal hajmi bir AQSH dollarida tengdir.

Mayning jarayonini boshlashdan avval, **RDP**-servisda qanday kriptovalyuta mayningi bilan shug'ullanishingizni hal qilib olishingiz kerak bo'ladi. O'z xoxishingizga ko'ra, bitkoin, dogikoin, bitcash, ethirium yoki laytkoinni tanlashingiz mumkin. Agarda yangi hisoblash quvvatlari sotib olsangiz, elektron hamyoningiz yanada tezroq virtual pullarga to'la boshlaydi. Virtual pullarni tizimdan chiqarib olish uchun foydalanuvchi o'zining virtual hamyoni nomerini korsatishi kerak bo'ladi. Pullarni tizimdan chiqarish bir necha kun davomida amalga oshadi.

Shuni ham qo'shimcha qilish lozimki, mablag' sarf qilmasdan turib virtual pullarni mayning qilish qonun bo'yicha ta'qiqlanmagan, ammo bunda keyinchalik firibgarlarning tuzog'iga tushib qolmaslik chora-tadbirlarini ko'rib qo'yish maqsadga muvofiq bo'ladi. Avvalo tegishli forumlar orqali u yoki bu mayning loyihasi haqida ma'lumotlar yig'ish va tegishli hulosalar chiqarish kerak bo'ladi. Shuni ham aytish kerakki, katta mablag' sarf qilmasdan turib kriptovalyutalar generatsiya qilish uchun eng ma'qul variant bulutli taxnologiyaga asoslangan mayning hisoblanadi. Internetda ajratilgan bonus tufayli kriptovalyutalar mayningini boshlang'ich pul mablag'lari sarf qilmasdan turib boshlashga imkon beradigan bir qancha imkoniyatlar mavjud, ular jumlasiga **XMine**, **Multi-Coin**, **AroMine**, **BiteMiner** va **Bit-Lite** larni kiritish mumkin. Bularda ham foydalanuvchu daromadi miqdorini ko'paytirish uchun o'z shaxsiy pullariga hisoblash quvvatlari sotib olishi ham mumkin. Agarda foydalanuvchi puldor bo'lsa, u kriptovalyutalar mayningi uchun biror bir sifatli dastur sotib olishi va solo-mayningni amalga oshirishi mumkin.

### ***5. Turli kriptovalyutalar va ularning tavsifi***

**Litecoin (Laytkoyn)** deb nomlangan kriptovalyuta dunyodagi eng ommalashgan kriptovalyutalar turlaridan biri hisoblanadi. Litecoinning maxsus yaratilgan saytida uni ko'pincha «*raqamli valyuta*» deb ham ataylaydilar. Litecoin uni yaratuvchilar tomonidan asosiy raqamli valyuta bo'lgan **Bitcoin**ning evolyutsiyasi hisoblansada, undan ancha-muncha farq ham qiladi. 2013 yilning 11

dekabri xolatiga ko'ra **BTC-E** birjasida 1 **LTC** taxminan 33 AQSh dollariga teng hisoblangan. Laytkoinlar pul almashtirish shaxobchalarida bitkoinga yoki oddiy pullarga almashtirilishi mumkin. Undan tashqari, kriptovalyutalar turli xil tovar va xizmatlarni sotib olish uchun ham ishlatilishlari mumkin (*agarda sotuvchilar bunga rozi bo'lsalar, albatta*). Laytkoin o'zining bir qancha ko'rsatgichlari bilan Bitkoinga juda ham o'xshab ketadi. Bular jumlasiga quyidagilarni kiritishimiz mumkin:

- Mayning pullar topishning asosiy vositasi;
- Tarmoqning markazlamagani va tarqoqligi;
- Tashqi nazoratning mavjud emasligi;
- Emissiyaning algoritmik jihatdan chegaralanganligi;
- Pul mablag'lariga **anonim** jihatdan egalik qilish va ulardan foydalanishning anonimligi (*bunga tranzaksiyalar ham kiradi*);
- Tranzaksiyalarni rad etishning mumkin emasligi;
- Mablag'larni tarmoqning bir qismi bo'lgan **hamyon** faylida saqlanishi.

Xuddi Bitcoin kabi, Litecoin ham **C++** tilida yozilgan va mijoz uchun Windows, Mac OS X, Linux versiyalarida saqlanadi.

### **LITECOIN (LTC) ning BITCOIN (BTC) dan asosiy farqlari:**

- Litecoin hisoblash amallari uchun markaziy protsessorni Bitcoin ga nisbatan samaradorroq ishlatadi, mayningning afzalliklari esa unda biroz pastroq darajada bo'ladi.
- Pul o'tkazmalarini tasdiqlash uchun to'rt marta kamroq vaqt sarfi kerak bo'lishi;
- Pul mablag'larining maksimal katta miqdoridan foydalana olish mumkinligi – ya'ni 84 million dollar;
- Har 3,5 kunda kriptografik hisoblarning murakkablik darajasi qayta hisoblanilib turiladi;
- Tarmoqda jami bo'lib 84 million **LTC** dan foydalanish mumkin, bu esa **BTC** ga nisbatan to'rt marta ko'p deganidir;

- Yangi bloklar generatsiya qilingani uchun mukofotlanuv ham 840 000 blokdan so'ng ikki baravarga kamaytiriladi;
- Laytkoinning loyihachilari o'zlarining asosiy maqsadlari sifatida bitkoin tizimidagi xatolar va kamchiliklarni tuzatishni qabul qilganlar. Kriptovalyutalar bilan ish olib borilganida Litecoining kursi Bitcoining kursiga bog'liq ekanligi kuzatiladi. Bu ularning bir biriga bog'liqligidan emas (*chunki ular bir-biriga bog'liq bo'lmagan valyutalar*dir), balki Bitcoin va Litecoinga bo'lgan talab va taklifning o'zaro balansi natijasida paydo bo'ladi. Kriptovalyutalarning kurslarini umuman bashorat qilib bo'lmaydi va xolat istalgan daqiqada batamom o'zgarib ketishi mumkin. Ayniqsa bu xolat 21 million bitkoinlar ishga tushib ketgandan so'ng yaqqol kuzatiladi.

*Laytkoinlarning keyingi vaqtda kuzatilgan katta muvaffaqiyati quyidagilarda deb ta'kidlashimiz mumkin:*

1. **Kipr** davlatining o'z iqtisodiyotining ayrim qismlarni bitkoinlarga o'tkazishni rejalashtirganligi;
2. Kriptovalyutaga juda katta pullar oqimining kirib kelganligi. Ularning kapitalizatsiyalashuvi bir milliard AQSH dollaridan oshib ketdi;
3. Ko'pchilik insonlarning 100 sumga ham, 3 dollarga ham bitkoin sotib oloilmaganliklari ularning bitkoin millionerlari bo'lish imkoniyatlarini batamom yo'qqa chiqarganligi;
4. Shuning uchun ham bitkoindan keyingi ikkinchi alternativ kriptoalyuta – laytkoinning obrusi orta boshladi. Ushbu bozorda faoliyat ko'rsatayotgan ko'pchilik insonlar laytkoin ham bitkoinning muvaffaqiyatini qaytarishiga va u ham 1000 dollargacha kattalikka o'sa olishiga ishonidilar;
5. Kriptovalyutalarning asosiy birjasi o'zida laytkoinlardan ham foydalanishini bildirdi;
6. Yuqoridagi sabablar tufayli ko'pchilik laytkoinlarni faol ravishda sotib ola boshladilar.

Xozirgi davrdagi asosiy kriptoalyutalarning qisqacha tavsifi quyidagi jadvalda keltirilgan:

AYUPOV R.H., KABULOV V.K.

<i>Valyuta</i>	<i>Kod</i>	<i>Yaratilgan vaqti</i>	<i>Muallif</i>	<i>Faollik</i>	<i>Sayt</i>	<i>Xesh</i>	<i>Izox</i>
Bitcoin	BTC	2009	Satoshi Nakamoto	Ha	bitcoin.org	SHA-256	Birinchi va eng ommabop kriptovalyuta, proof-of-work
Litecoin	LTC	2011	Coblee	Ha	litecoin.org	Scrypt	proof-of-work
Namecoin	NMC	2011	Vinced	Ha	dot-bit.org	SHA-256	proof-of-work. Markazlashmagan DNS sifatida, internet-tsenzurani qiyinlashtirish maqsadida

Kriptovalyutalarning baʼzi bir xususiyatlarini va internet manzillarini quyida qisqacha tavsiflab oʻtamiz:

### **LTC (<http://litecoin.org>) - Litecoin**

Ushbu kriptovalyuta ommaviyligi jihatidan ikkinchi oʻrinda turadigan kriptovalyutadir. Unda bloklar har 2,5 daqiqada generatsiya qilinadi va unda 84 million pul birligi mavjud. Tizimning murakkabligi har bir 2016 blokda oʻzgarib turadi (3,5 kunda) va har bir blok uchun mukofotlanuv – 50 LTC har 840 000 blokda ikki barobar kamayadi. Xeshlashtirish algoritmi «scrypt» turiga mansub. Ushbu algoritmnining boshqalaridan asosiy farqi **LTC** ning markaziy protsessorda osonroq mayning qilinishidir. Bular haqida **Litecoin** ning maʼlumotnomasida va mayning bʼyicha qoʻllanmada batafsilroq keltirilgan.

### **NMC (<http://namecoin.info>) - Namecoin**

Namecoin kriptografik jihatdan himoyalangan va **.bit** deb nomlangan domen zonasida ishlash uchun yaratilgan. Ushbu «**valyuta**» Bitcoin kontseptsiyasiga asoslangan boʻlib, u bilan bir xilda hisoblanilishi mumkin. Pullarning oʻzi **.bit** zonasidagi domenlarni qayd qilishga asoslangan. Bitcoin kriptografik tizimchasi tufayli bunday domenlar ularning egalaridan boshqalar tomonidan oʻzgartirishga qarshi himoyalangan. Ammo DNS-serverni oʻz shaxsiy kompyuterida koʻrib chiqish imkoniyati har bir ishtirokchi uchun mavjud.

### **PPC (<http://ppcoin.org>) - PPcoin**

**POW & POS** ning gibril dizayni xuddi shu valyutada amalga oshirilgan. Bu tizimda tranzaksiya 520 marta tasdiqlashni so'raydi, ammo pullar hamyonda darrov paydo bo'ladi. Tizim xakerlar xujumiga anchagina chidamli hisoblanadi.

#### **NVC (<http://novacoin.org>) - Novacoin**

Novacoin tizimini yaratishdan asosiy maqsad **PPCoin** larning afzalliklarini yana bir marta qaytarish bo'lgan. Ammo bunda uning juda ham katta emissiya xajmi kabi kamchiliklaridan qutulishga harakat qilingan. NVC o'zida xeshlashtirish algoritmi sifatida Scrypt funksiyasidan foydalanadi. Emissiyaning chegaraviy tezligi 100 martagacha kamaytirilgan, murakkablik oshishi bilan mukofotlanishning kamayish tezligi esa qiyaligi biroz kamroq bo'lgan chiziqli bilan amalga oshirilgan. **PPCoin** loyihasiga o'xshash, murakkablik tarmoqning har bir blokida qaytadan hisoblanadi. Har bir hisob-kitobda murakkablikning oshishining maksimal kattaligi 1% ni tashqil qiladi. Tarmoqlardagi bloklarni generatsiya qilishning maqsadli tezligi soatiga 6 blokni tashqil qiladi.

#### **TRC (<http://terracoins.org>) - Terracoin**

Bu tizimda bloklar har 2 daqiqada generatsiya qilinadi va jami tizim tangalari soni 42 millionni tashkil qiladi. Murakkablik esa har 30 blokdan keyin qayta hisoblanadi. Blok uchun mukofotlanuv 20 **TRC** deb belgilangan. Har 1 050 000 blokda mukofotlanuv ikki barobar kamayadi.

#### **FTC (<http://www.feathercoin.com>) - Feathercoin**

Feathercoinlar - fork Litecoin hisoblanadi va u scryptdan hamda POW sxemadan foydalanadi. Bloklar har 2,5 daqiqada generatsiya qilinadi. Unda jami 336 million tanga mavjud. Murakkablik har 5040 blokda qayta hisoblanadi, blok uchun mukofot miqdori 200 **FTC** bo'lib, u har 8 400 000 blokda ikki marta kamayadi.

#### **CNC (<http://chncoin.org>) - Chinacoin**

Chainacoin ham fork Litecoin hisoblanadi va u scryptdan hamda POW sxemadan foydalanadi. Bloklar har bir daqiqada generatsiya qilinadi. Unda jami 2 628 000 bloklar bo'lib, u 462,5 million tangani tashqil qiladi. Murakkablik har 5040 blokda qayta hisoblanadi, blok uchun mukofot miqdori 88 **CNC**.



### **RUC (<https://www.rucoin.org>) - Rucoin**

Ushbu kriptovalyuta tangalarni scrypt hamda **sha256d** sxemalari orqali generatsiya qiladi. Tarmoqning xakerlar xujumidan himoyalaniş kattaligi 51% ga teng bo'lib, u mayningda generatsiya qilingan bloklarning katakchalari nomi bilan amalga oshirilgan. Xakerlar xujumi vaqtida tarmoq himoyalangan rejimga o'tadi va bloklarni faqatgina ishonchli tugunlardangina qabul qila boshlaydi. Hamyonlarning nomlari chiroyli va tranzaksiyalar izoxlar orqali keltiriladi.

Konfidentsial to'lovlar uchun kriptografiyaning ilk bora ishlatilishi 1990 yildan **Devida Chomning DigiCash** tizimidan boshlangan. Afsuski, uning kompaniyasi 1998 yilda bankrotlikka uchragan. Ammo uning to'lov tizimi markazlashgan bo'lgani uchun saqlanib qolgan va «kriptovalyuta» atamasi birinchi marta Bitcoin pirring to'lov tizimi paydo bo'lganidan so'ng ishlatilina boshlandi. Ushbu tizim 2009 yilda Satoshi Yakomoto ismli (*psevdonomli*) inson yoki shaxslar guruxi tomonidan ishlab chiqilgan. Bu tizim **SHA-256** turidagi xeshlashtirishdan va proof-of-work tizimidan foydalanadi. Shundan keyingi yillarda Bitcoin ga bog'liq bo'lmagan mustaqil kriptovalyutalar ham ishlatilina boshlandi. Ularni Bitcoin forklari deb ataladi. Masalan, Namecoin, Litecoin, PPCoin, Novacoin va boshqalar. Bulardan boshqa bir qancha forklar ham yaratilgan, ammo ularning Bitcoindan unchalik katta farqlari yo'q desa ham bo'ladi. Farqlari faqat emissiya tezligi va chegaralari yoki xesh-funktsiyalar algoritmlaridagina bo'lishi mumkin. Bunday turdagi ko'pgina forklar 2011-2014 yillarda Bitcoinning bozorda erishgan muvaffaqiyatlari tufayli vujudga kelgan deyishimiz ham mumkin. Kriptovalyutalarning boshlang'ich narxi uning generatsiya qilish uchun kompyuterga sarf qilingan elektr energiyasining bahosiga teng deyish mumkin. Kriptovalyutaning ikkilamchi bozoriy narxini esa unga bo'lgan talab aniqlab beradi. Bunday talab ikki xil turda bo'lishi mumkin:

- 1) spekulativ — investorniki (*kriptovalyutani uni yanada qimmatroq sotish maqsadida sotib olish*);
- 2) Kriptovalyuta to'lab, o'rniga qandaydir tovar yoki mahsulot olish;

3) Kriptovalyutani boshqa hisob raqamiga komissiyasiz (*yoki 0,1% dan ham kamroq komissiya bilan*) o'tkazish.

Bulardan tashqari, kriptovalyutaning bozoriy narxini xosil qilishda uning oxirgi emissiyasi qanday bo'lganligi ham ro'l o'ynaydi. Bitcoin tarmog'ini yaratgan Gevin Andrisen ham ba'zi bir kriptovalyutalarning firibgarlik mahsuli bo'lishi mumkinligidan o'z xavotirini bildirgan. Xozirgi davrda Bitcoindan boshqa hech qanday kriptovalyuta bunchalik keng miqyosda tarqalmaganligini ham aytib o'tishimiz kerak. Litecoin va Namecoin kriptovalyutalari boshqalarga nisbatan biroz kengroq tarqaldilar, ammo Bitcoinga yetishning uddasidan chiqa olmadilar. Boshqa barcha kriptovalyutalar ularning kurslarida biroz miqdorda spekulyatsiya qilish uchun ishlatiladilar va boshqa yerlarda ishlatilganlari xozircha kuzatilmadi. Asosiy kriptovalyutalar emissiyaning quyidagi umumiy miqdori doirasida amal qiladilar: **(BTC) Bitcoin** — 21 million kriptotanga va **(LTC) Litecoin** — 84 million kriptotanga.

Kriptovalyutalar bilan ishlashni boshlashni o'rganish yoki ular bilan ishlashga mo'ljallangan saytlar soni va kriptovalyutalar birjalari juda ham ko'p miqdorda. Masalan, **BTC - e** birjasi, **Exmo.com** - birjasi, **LiveCoin.net** - zamonaviy birjasi, **CEX.IO** - birjasi, **eCoin.eu** - birjasi, **GOC.io** - kriptovalyutalar bilan avtomatik tarzda savdo qiluvchi platforma, **Cryptonit.net** kriptovalyutalar sotuvchi va sotib oluvchi birjasi, **Kraken** kompaniyasining birjasi, **Bitfinex** - AQSh dollari bilan savdo qiluvchi eng katta birjasi, **BTC China** - savdo xajmi bo'yicha dunyodagi eng katta Xitoy firmasi, **BitYes.com** - AQSh dollari bilan katta miqdordagi savdo xajmini amalga oshiruvchi Xitoy kriptovalyuta birjasi va boshqalar. Keyingi paytda rusiyazon foydalanuvchilar uchun mo'ljallangan kriptovalyutalar bilan avtomatik tarzda savdo qiladigan tizimlar ham tobora mashxur bo'lib bormoqda. Ularga bir marta kirasiz va unga a'zo bo'lganingizdan so'ng, savdo jarayonini tizimning o'zi avtomatik tarzda amalga oshiradi. Siz ham o'z omadingizni ushbu kriptovalyuta savdo tizimlarida bimalol tekshirib ko'rishingiz mumkin. Ammo savdo jarayonini boshlashdan avval kriptovalyuta turlarini va savdo amaliyotini mavjud trenajerlarda yaxshilab o'rganib, o'zlashtirib

AYUPOV R.H., KABULOV V.K.

olishingizni maslaxat qilar edik. Quyidagi tasvirda kriptovalyutalar olami o'ziga xos mozaikali tasvirlar vositasida keltirilgan va u kripto-olam to'g'risidagi o'quvchi tasavvurini yanada boyitish uchun xizmat qiladi:



Yuqorida aytilganlardan kelib chiqqan xolda shuni aytish kerakki, raqamli valyuta deganda shunday valyuta turiga aytiladiki, bunday turdagi valyuta hozirgi paytda hamyoningizda bo'lgan qog'oz ko'rinishidagi valyutalardan farqli o'laroq, faqatgina electron ko'rinishda bo'ladi. Ammo, hozirgi davrda ko'pchilik insonlar bitkoin, laytkoin, token va blokcheynlar kabi electron valyuta turlaridan qanday foydalanishni tushunavermaydlar. Demak, tabiiy ravishda quyidagi savol tug'iladi: Elektron valyutalar vositasida internet tizimi orqali odatiy pul kabi to'lovlar amalga oshirish mumkinmi? Quyida shu va shu bilan bog'liq bir qancha dolzarb savollarga javob berishga harakat qilamiz.

### ***Kriptovalyutalarning turlari, ularning bozor kapitalizatsiyasi va izohlar***

Valyuta turi	Kodi	Yili	Muallifi	Faoli- ligi	Sayti	Maksimal qo- ri	Bozor kapitalizat siyasi (2017 yil oktabr holatiga mln.AQSH dollarida)	Xe- sh	Izoh
--------------	------	------	----------	----------------	-------	-----------------------	---	-----------	------

Valyuta turi	Kodi	Yili	Muallifi	Faoligi	Sayti	Maksimal miqdori	Bozor kapitalizat siyasi (2017 yil oktabr holatiga mln.AQSH dollarida)	Xesh	Izoh
<a href="#">Bitcoin</a>	BTC, XBT	2009	<a href="#">Сатоши Накамото</a>	Ha	<a href="http://bitcoin.org">bitcoin.org</a>	21 mln	89 592	<a href="#">SHA-256</a>	Birinchi va eng mashhur kriptovalyuta, proof-of-work
<a href="#">Ethereum</a>	ETH	2015	<a href="#">Виталик Бутерин</a>	Ha	<a href="http://ethereum.org">ethereum.org</a>		28 840	Ethash	
<a href="#">Ripple</a>	XRP	2005, 2011	Ripple Labs Inc.	Ha	<a href="http://ripple.com">ripple.com</a>		8 312		To'lov tizimi, raqamli aktivlar birjasi va kriptovalyuta.
Bitcoin Cash	BCH	2017	Fork block 8MB	Ha	<a href="http://www.bitcoincash.org">www.bitcoincash.org</a>	21 mln	5 391	<a href="#">SHA-256</a>	proof-of-work
<a href="#">Litecoin</a>	LTC	2011	Coblee	Ha	<a href="http://litecoin.org">litecoin.org</a>	84 mln	3 067	<a href="#">Scrypt</a>	proof-of-work
Bitshares	BTS	2014	Daniel Larimer	Ha	<a href="http://bitshares.org">bitshares.org</a>	2,6 mlrd + zaxira ~1 mlrd	140		Delegated Proof of Stake (DPoS)
<a href="#">Peercoin</a>	PPC	2012	Sunny King	Ha	<a href="http://ppcoin.org">ppcoin.org</a>	Yuqori miqdori mavjud emas	27	SHA-256	<a href="#">proof-of-work/proof-of-stake</a> gibrid mexanizmi
<a href="#">NXT</a>	NXT	2013	BCNext	Ha	<a href="http://nxt.org">nxt.org</a>	1	13		<a href="#">proof-of-stake</a>

Valyuta turi	Kodi	Yili	Muallifi	Faoli gi	Sayti	Maksimal miqdori	Bozor kapitalizat siyasi (2017 yil oktabr holatiga mln.AQSH dollarida)	Xesh	Izoh
						mlrd			
<a href="#">Namecoin</a>	NMC	2011	Vinced	Ha	<a href="#">dot-bit.org</a>		11	SHA-256	proof-of-work

Shuni ham aytish kerakki, bitkoin tangalarini yaratish uchun sarflanadigan xarajatlar unchalik katta emas, biroq xuddi oltin yoki neftni qazib olishdagi tashkilotlar ko'payishi va ushbu resurslarning kamyob topilishi bois narxi oshgani singari bitkoinni ham so'nggi vaqtlarda mayning orqali hosil qilish murakkablashgan holda butun bir boshli «mayning fermalari»dagi bir necha kunlik to'xtovsiz amaliyot natijasida bor yo'g'i bir nechta bitkoin hosil bo'layotgani hamda bitkoinlar maksimal soni chegaralangani (21 000 000) narxning ko'tarilishiga turtki bo'lmoqda. Biroq bundan boshqa yana eng katta sabablardan biri bitkoinni Xitoy, Yaponiya va Janubiy Koreya singari rivojlangan mamlakatlar iqtisodiyotida rasman to'lov vositasi sifatida qabul qilinishi ushbu bitkoin tangalariga nisbatan talabni chunonan kuchaytirdiki, 2017 yilning o'zida yil boshiga nisbatan jadal o'sish ko'rsatkichiga erishildi (kurs 998 AQSh dollaridan 20000 AQSh dollarigacha o'sdi). Bugun dunyodagi yetakchi birjalar va yirik banklar ham bitkoinning oldi-sotdisini treyding tizimida yo'lga qo'yishlariga to'g'ri kelmoqda. Garchi kriptovalyutalarning gurkirab rivojlanishi butun jahon moliyaviy-iqtisodiy tizimiga katta ta'sir qilgan holda mavjud bo'lgan tizimni yo'q bo'lib ketishiga sabab bo'lishi mumkin bo'lsa ham, ayni paytda katta daromad ko'rish istagida bo'lgan investorlar bitkoinning rivojlanishidan manfaatdor bo'lishmoqda. Shuningdek, bitkoin tangalarini gurkirab rivojlanishidan eng ko'p manfaat ko'ruvchi insonlar – bu yashirin iqtisodiyotda faoliyat yurituvchi

investorlardir. Aynan shuning uchun ham hozirda bir nechta iqtisodiy rivojlangan davlatlar bitkoin orqali turli noqonuniy va jinoiy faoliyatlarning rivojlanib ketishi oldini olish maqsadida bitkoinni to'lov vositasi sifatida qabul qilishmayapti.

Bitkoinni xarid qilish masalasiga to'xtaladigan bo'lsak, hozirgi vaqtda uni bir nechta maxsus birjalar va umuman har qanday bitkoinga ega bo'lgan ishtirokchidan to'g'ridan-to'g'ri sotib olish yo'llari mavjuddir. Unda bitkoinning qiymati ishtirokchilar o'zaro kelishgan narxda amalga oshiriladi. To'lovlar agar birjalar orqali amalga oshirilsa, xalqaro VISA, Master Card kartalari orqali va Webmoney, Qiwi, Perfect Money, Advcash, Payeer, Paypal va boshqa elektron hamyonlar orqali sotib olish mumkindir.

Hozirgi kunga kelib, kriptovalyutalarga ma'lum bir usulda (*mayning, forjing*) emissiyasi qilganlarga ularga ega bo'lishi mumkin. Qolganlar esa virtual pullarni faqatgina boshqalardan olishlari mumkin. Buning uchun ma'lum miqdorda pul to'lashlari yoki tovar yoki xizmatga almashtirishlari mumkin. Almashinuv hech qanday vositachilarsiz amalga oshirilishi mumkin. Ammo amaliyotda bu ishni maxsus joylardagina amalga oshirish mumkin bo'lib qolmoqda. Bu esa tabiiy ravishda kriptovalyutalar bozorini vujudga keltirdi. Natijada hozirgi vaqtda kriptovalyutalar egalari ularni nafaqat haqiqiy pullarga balki boshqa turdagi virtual pullarga ham almashtirish imkoniga ega bo'lmoqdalar.

## ***6. Kriptovalyutalardan foydalanish muammolari***



Birinchi navbatda, shuni tushunish lozimki, siz O'zbekistonda bitkoinlarga nimanidir rasman harid qila olmaysiz, ya'ni harid uchun hech kim sizga to'lov cheki bermaydi. Bitkoinlar bilan to'lov qilish mumkinligini e'lon qilayotgan sanoqsiz qahvaxona va savdo markazlari shunchaki mijozlarni jalb qilishni ko'zlashi ehtimoli yuqori — ya'ni ular bitkoinni barmen karmoniga o'tkazishingiz hisobiga sizga qahva sovg'a qilishi mumkin. Ammo, electron pullar, masalan, bitkoinlar qora bozorlarda tez-tez ishlatiladi. U to'lovlarning tez, anonim va nisbatan xavfsiz usuli hisoblanadi. Aynan shuning uchun ham ko'pchilik insonlar bunday harid usulini va bitkoinlardan foydalanishni qonunga xilof deb o'ylaydilar. Negaki ular joriy qonunchilikda to'liq aks ettirilmagan va xuddi shuning uchun ham ularning aylanmasi uchun javobgarlikni hech kim zimmasiga olishga tayyor emas. Biroq kriptovalyutalar bo'yicha tegishli qonun loyihalari qabul qilinishi bilan vaziyat tubdan ijobiy tomonga o'zgarishi mumkin. Shu tufayli quyidagi savol paydo bo'ladi: U holda nima uchun bitkoinlarni harid qilishadi? Birinchidan, ba'zi mamlakatlarda (*masalan, Yaponiya, AQSH va Yevropaning ba'zi mamlakatlarida*) bitkoinlar yordamida to'lovlar qilish — masalan, qahva yoki ko'chmas mulkni osongina va qulay usulda harid qilish mumkin. Mablag'ingiz o'sha zahoti eng minimal ustama-komissionlar bilan sotuvchiga yetib boradi va muhimi — bitimni amalga oshirish uchun sizga bank xodimlari yoki brokerlar kabi vositachilar talab



qilinmaydi. Bu esa pul o'tkazmasini yengillashtirib, uning anonimligini ta'minlab beradi (*chunki electron kriptovalyutaning hamyonlari uning egasi ismi bilan bog'liq bo'lmaydi*). Ikkinchidan, ko'pchilik insonlar ushbu usulni o'z jamg'armasining diversifikatsiyasi deb tushunadi. Elektron valyutalarning qiymati ham ko'pchilik holatlarda oshib boradi — har bir kishi valyuta kursi ko'tarilishi hisobidan mo'maygina daromad qilishga umid qiladi, albatta. Ho'p electron pullarning o'ziga hos afzalliklari bor ekan, ularni qayerlardan olish mumkin? Odatda internet-pul-ayirboshlovchilar, messenjerlardagi maxsus botlar, internet hamyonlar va kriptovalyuta birjalaridan foydalanishadi. Elektron pullardan foydalanishning qulayligi tufayli va valyuta kursi oshib borayotgan vaziyatda ularni harid qilishga talab borgan sari oshib bormoqda. Insonlar elektron pullarni, misol uchun, yaqin do'stlaridan, bu soha bo'yicha mutaxasislardan, tadbirkorlardan yoki uzoq-yaqin tanishlaridan harid qilishlari mumkin. “Yandeks” tizimidagi ba'zi pul ayirboshlovchilar bitkoinlarning bozordagi narxi 12300—12400 dollar chegarasida bo'lishiga qaramasdan, bitkoinlarni 13000 ming dollarga harid qilishni ham taklif qilishadi. Xozirgi kunlarga “**Kivi**” va “**Yandeks**” hamyonlaridan o'tkazmalarni amalga oshirishda aksariyat kriptovalyuta birjalarining komission to'lovlari besh foizgacha yetadi. Britaniyalik jurnalist Jun Yan Von Shveytsariya tog'larida joylashgan mahfiy bunkerda bo'ldi – bu yerda “**Haro**” kompaniyasi o'z mijozlarining bitkoinlari kriptografik kalitlarini saqlaydi:





Nazariy jihatdan qaraganda, electron valyuta sotib olishning eng oddiy va arzon usuli — joriy davrdagi eng foydali kurs bo'yicha harid uchun yirik kriptovalyuta birjasiga bank o'tkazmasini amalga oshirishdir. Ammo amalda bu jarayon bir qancha ob'ektiv va sub'ektiv sabablarga ko'ra, ancha murakkab hisoblanadi. Ko'pchilik banklar bu kabi bitimlarga juda ham salbiy va ehtiyotkorona munosabatda bo'ladlar. Juda konservativ xolatda bo'lgan banklar esa yuqori texnologiyalar olamiga qiziqishingizni bilib qolishsa, sizning tabiatingizni aniqlash uchun va extiotkorlik asnosida hatto hisob raqamingizni vaqtincha yopib qo'yishlari ham mumkin. Sizni va hisob raqamingizdagi mablag'lar harakatini maxsus vosilarni jalb qilgan xolda tekshiruv jarayoni haqida esa gapirma ham bo'ladi. Ho'sh, electron pullarning, shu jumladan, bitkoinning joriy kursiga nimalar ta'sir qilishi mumkin? Bitkoin bejizga raqamli oltin deb atalmaydi — uni chiqarish va tizimda yangi tangalarning paydo bo'lishi doimiy ravishda qisqarib bormoqda va matematik formula bilan cheklangan (*mutaxassislaening fikrlariga ko'ra, 2034-yilga kelib bitkoinlarning 99 foizi chiqariladi*). Talabning oshishi bilan narxlar ham o'sib borishi lozim. Boshqa tomondan qaraganda, hozirgi paytda bozorda tizimda foydalanish mumkin bo'lgan tangalarning 10 foizi bilangina faol savdo qilinmoqda. Shuning uchun kursning keskin oshib ketishini birjaga yangi bitkoinlar oqimini jalb etish bilan qoplash mumkin. Bu bilan bog'liq bir savol hosil bo'ladi: Bitkoinlar kursi deyarli har doim o'sib borishi ta'kidlanmoqda. Bir nechta bitkoin harid qilib, bir yildan so'ng boyib ketish mumkinmi? Buning ehtimoli ancha yuqori, biroq har doim navbatdagi o'sish oldidan kursning ikki-uch barobar tushib ketish xavfi mavjud. Shuning uchun yangi yil sovg'alarida daromad qilishga umid qilayotgan bo'lsangiz, siklga tushmay qolishingiz mumkinligini inobatga oling. 2017-yilning boshidan buyon bitkoin deyarli yigirma martadan ko'pga, efirium (*kapitalizatsiya bo'yicha ikkinchi o'rinda turuvchi valyuta*) esa 48 marta oshdi. Biroq keyinroq efirium qiymati ikki barobarga tushdi. Sabrli investor uchun daromad istiqboli ancha yuqori bo'lishi mumkin. Maqola yozilayotgan paytda barcha kriptovalyutalarning jahon kapitalizatsiyasi 85 milliard dollarni tashkil etgan. Shu sababdan bozorning yanada

o'sishi uchun barcha imkoniyatlar mavjud. Taqqoslash uchun: Rossiya aholisi bank depozitlari hajmi — 405 milliard dollar, AQShda bu ko'rsatkich — 9 trillion dollar. Qimmatli qog'ozlar dunyo bozori kapitalizatsiyasi esa 86 trillion dollar (2016-yil yakunida).

### **7. Blokcheynlar hamda ICO ning iqtisodiyotda ishlatilishi**

Endi blokcheynlarning iqtisodiy ahamiyati haqida ham biroz to'xtalib o'tamiz. Ko'pincha "*Blokcheyn — ma'lumotlarni saqlash uchun taqsimlangan reyestr...*" deb tushuntiriladi. Ushbu izohni bir necha marta eshitgan, biroq hech narsani tushunmagan bo'lishingiz mumkin. **Blokcheyn** — bir-biri bilan internet orqali bog'langan ko'plab kompyuterlarda bir vaqtning o'zida saqlanuvchi ma'lumotlar bazasi. Uning nega kerakligini misol yordamida tushuntirish osonroq. AQSh dagi akangizga bank jo'natmalari orqali 100 dollar yubordingiz deb tasavvur qiling. Jo'natma shaklini to'ldirganingizdan so'ng bank xodimi shaxsiy hisobingizdan pulni yechib olib, uni xalqaro o'tkazmalar uchun bankning yagona hisobiga o'tkazadi. Shundan so'ng boshqa xodim bu pullarni agent bankning hisobiga o'tkazadi, u esa, o'z navbatida, pullarni AQSh ga o'tkazadi. U yerda o'tkazmangiz aynan shu taxlit akangizning shaxsiy hisobiga tushadi. Jo'natma davomida hech kim xatoga yo'l qo'ymagan bo'lsa, uch kun o'tib akangiz 97 dollarni oladi (*barcha banklarning komissionlari olingandan so'ng*). Biroq eng qo'rqinchlisi, shu uch kun ichida na siz va na sizning akangiz, qolaversa, bankirlardan hech biri ayni vaqtda pullaringiz qayerda ekanligi va ularning hisobini kim yuritayotganligini bilmaydi. Serverning kutilmaganda buzilib qolishi, bank xodimining insofsizligi yoki xakerlik hujumi uzoq surishtiruvlarning boshlanishiga sabab bo'lishi mumkin. Axir bu kabi hodisalar hisobingizdagi pullar bilan ham sodir bo'lishi mumkin. Demak, siz har kuni tizimga umid qilasiz va bankingizga ishonasiz, bu esa katta muammo. Hozirda blokcheynlar asosan kriptovalyuta jo'natmalari uchun foydalanilmoqda. Biroq u turli tashkilotlarning turli maqsadlari uchun ham faol joriy etilmoqda. Blokcheynning afzalligi uning shaffof, tezkor, soddaligi va qiymatida. Siz kriptovalyuta yoki biror ma'lumotni

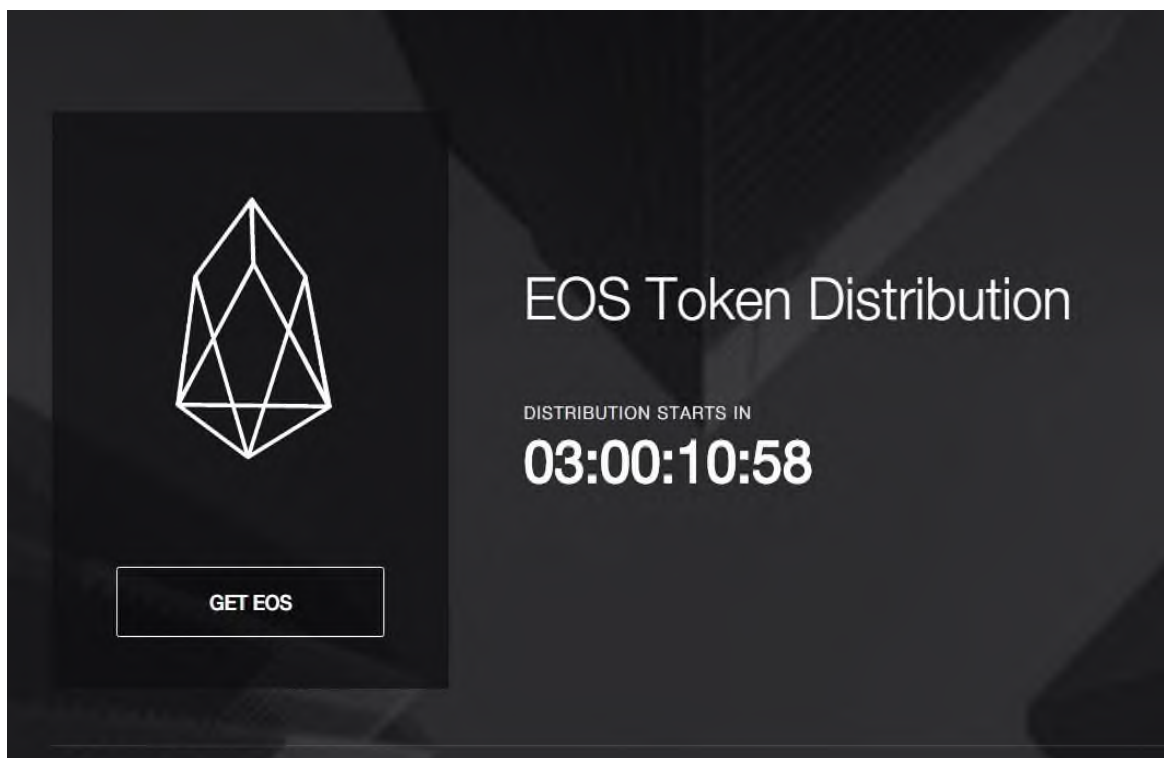
blokcheyn orqali jo‘natgan bo‘lsangiz, bunday jo‘natma haqida ma’lumotni o‘zgartirish yoki qalbakilashtirishning imkoni yo‘q. Chunki u butun dunyo bo‘yicha yuz minglab kompyuterlar tomonidan tasdiqlanadi. Aynan ushbu kompyuterlarda ushbu ma’lumotning ko‘plab nusxalari saqlanadi — ular bilan istalgan foydalanuvchi istalgan vaqtda tanishishi mumkin. Jo‘natma jarayoni bor-yo‘g‘i bir necha daqiqa vaqt oladi va bank jo‘natmasidan bir necha o‘n marta arzonidir. Agar siz pullar yoki ma’lumotni blokcheynda saqlasangiz ushbu qaydlar hech qachon yo‘qolib ketmaydi yoki soxtalashtirilmaydi. Bozorning istalgan ishtirokchisi istalgan daqiqada moliyaviy ahvolingizga ishonch hosil qilishi mumkin. Hech qanday uchinchi tomon yoki vositachi ishtirokisiz, to‘liq shaffoflik va hisoblar aniqligining matematik kafolati ta’minlab beriladi.



Endi **ICO** (*Initial Coin Offering - kriptovalyutani birlamchi joylashtirish*)) nimaligi haqida qisqacha ma’lumot berishga harakat qilamiz. Buni tushunish uchun attraksionlar parkini tasavvur qiling. Uning kirish qismida park emblemasi tushirilgan jetonni harid qilasiz va turli ko‘ngilochar o‘yinlar va attraksionlar uchun u bilan to‘lov qilasiz. Blokcheynlar bilan ishlovchi turli loyihalar (*masalan, ma’lumotlarni saqlashga ixtisoslashganlar*) ham ana shunday jetonlar chiqaradi. Ular tanga yoki **token** deb ataladi. Haridor ana shunday token harid qilib, uning

yordamida loyiha biror-bir xizmati, aytaylik, ma'lumotlar bazasidagi o'z saqlash joyi hajmini oshirish uchun to'lovni amalga oshiradi. Agar bunday loyiha ommalashsa, tokenlarning ham qiymati oshadi. Blokcheyn-loyihalar tokenlar chiqarganda, ularni odamlar harid qila olishi uchun bozorga joylashtiradi. Bu tanga - tokenlarni birlamchi joylashtirish — **ICO - Initial Coin Offering**dir.

**ICO** lar ichida eng taniqli bo'lganlardan biri **GNOSIS** deb nomlangan va u ishga tushurilgandan so'ng 15 daqiqa ichida 12 million dollarga ekvivalent bo'lgan mablag' yig'ishga erishgan. Ammo bu paytda u o'zining faqatgina 5% **GNO** tokenlarinigina chiqargan edi xolos. Bu degani, **GNOSIS 300** million potentsiyal dollarga teng tokenlar kapitalizatsiyasiga ega bo'lgan xolda, biror bir hayotchan tijoriy mahsulot ishlab chiqarmasdan turib, yaxshigina mablag'ga ega bo'lishidir. **GNOSIS** bo'yicha materiallarni o'rganish **ICO** ning tuzilishini, uning ishlashini, **GNO** tokenlarining qanday faoliyat ko'rsatishini va xaridor uchun foydasini tushunish imkonini beradi. *Gnosis Limited* kompaniyasining “*Tokenlarni sotish shartlari*” deb nomlangan xujjatda uning xuquqiy tomonlari har qanday moliyaviy instrument kabi juda chuqur yoritilgan, ammo undagi iqtisodiy tomonlar va murakkaliklar deyarli ko'rib chiqilmagan. Moliyaviy injiniring sohasidagi mutahassislar uchun ham bunday chalkash masalalarni chuqur o'rganib chiqish unchalik oson emas. Agarda tokenlar yangi kriptovalyutalarning tokenlari bo'lmasalar, **ICO** da foydalaniladigan tokenlarning kriptovalyutalar bilan hech qanday umumiy tomoni yo'q. Kriptovalyuta – ommaviy blokcheynning ichki hisob birligi bo'lsa, tokenlar – investorning kompaniya tomonidan pulga alishtiriladigan raqamli aktividir. Kriptovalyutani mayning yordamida topadilar, tokenlar emissiyasini esa uni chiqargan tashkilot amalga oshiradi. Kriptovalyuta bilan tokenning asosiy farqi shundaki, tokenda blokcheyn ham, hamyon ham yo'q, lekin kriptovalyutada bularning ikkalasi ham bor. **ICO** biror bir loyihaga pul jalb qilish uchun chiqariladi va sotiladi, pul to'lab kontrakt funksiyasini bajaruvchi tokenlar sotib olgan insonlarga esa tokenlar o'rniga nimadir berish taklif etiladi.



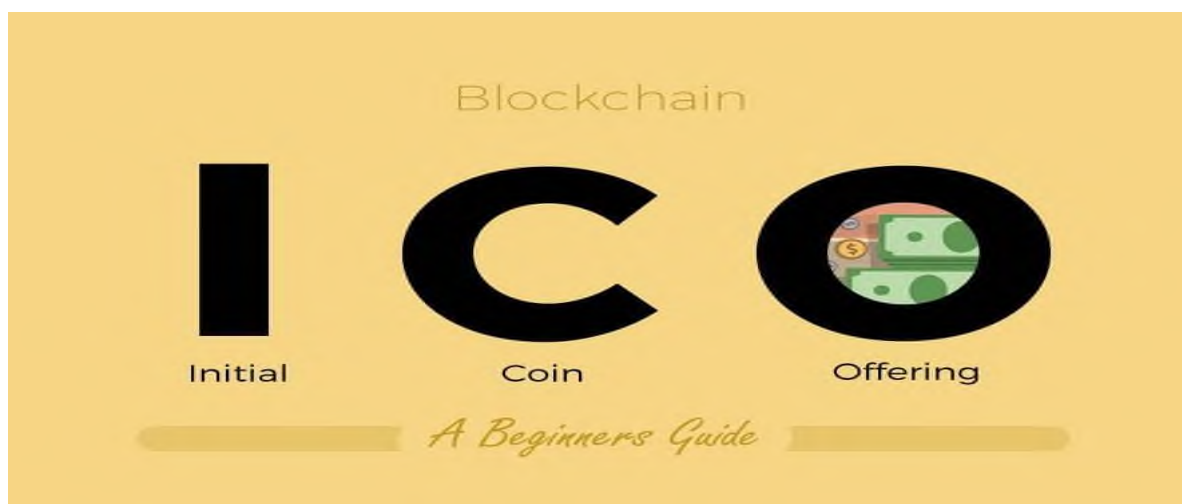
Demak, investor kriptovalyuta yoki tokenlar uchun kelajakda nimanidir olish huquqiga ega bo'ladi. Uning kelajakda nima olishi, startup loyihaning qanchalik muvaffaqiyatli chiqishiga bog'liq bo'ladi. Deyarli barcha **ICO** lar bir xilda amalga oshiriladi: tashkilotchilar elektron hamyonning adresini bildiradilar va ma'lum bir shartlar asosida unga pul jo'natishni taklif qiladilar. Mablag'lar yig'ilib bo'linganidan so'ng, investorlarning elektron hamyonlariga raqamli aksiyalarni jo'nata dilar. Tokenlar xaridorlarning **ICO** ga jo'natgan pullari miqdoriga proportsional ravishda taqsimlanadilar. Masalan:



### Распределение токенов

- **60%** покупателям токенов
- **28%** команде
- **10%** мотивация контрибьюторов
- **2%** советникам и партнерам, баунти

Tokenlarni birja orqali, **ICO** jarayonida yoki boshqa insonlardan sotib olish mumkin. Ba'zi xollarda **ICO** saytida registratsiya qilinish talab etilishi mumkin – shartlarga rozilik beriladi va tokenlar sotib olinadi. Shundan so'ng, tokenlar birjalarda turli narxlarda sotilishi mumkin, ammo hech qachon uning narxi ortadi deb ishnosh mumkin emas. Investorlar o'z tokenlarini birjalarga kiritishi va uni boshqa kriptoaktivlarga yoki an'anaviy valyutalarga almashtirishlari ham mumkin. Albatta token sotib olgan investor uni keyinchalik sotib foyda olishni yoki **ICO** tashkil qilgan kompaniya xizmatlaridan foydalanib, nimalargadir erishishni rejalashtiradi. Tokenlarni sotish uni sotib olingan joyida amalga oshirilishi yoki bunga qiziqqan haridorga sotilishi mumkin. Tokenlarni muomalaga chiqarish uchun mo'ljallangan mahsus platformalar ham mavjud, masalan, ularning ichida eng ommaviylari - **Ethereum, Waves, NEM, EOS** va **KickICO** lardir. Ularning har birining ijobiy va salbiy tomonlari mavjud. Masalan, **Ethereum** da eng katta auditoriya (*foydalanuvchilar soni 5 million*) bo'lsa, **Waves** da tokenlarni juda tezkorlik bilan chiqariladi, **KickICO** da esa **ICO** tashkil etish va uni amalga oshirish uchun tayyor uskunalari mavjud. Shuning uchun yangi tokenlar paydo bo'lishini **ICO**-chilar amalga oshiradigan platformalar orqali kuzatib turish ham mumkin. **ICO** larga qancha mablag' jalb etish maqsadga muvofiq bo'ladi degan savolga javob barcha turdagi yuqori tavakkalchilik darajasiga ega bo'lgan investitsiyalar kattaliklariga bo'lgan kabidir – ya'ni, **ICO** ga o'zingiz yo'qotib qo'yishdan qo'rqmaydigan summani investitsiya qilgan ma'quldir.



Yuqoridagilarni diqqat bilan o'qib chiqqanlarda kriptovalyutalarning yoki tokenlarning hammaga ma'lum va mashxur bo'lgan moliyaviy piramidalarga o'shab ketishini anglash mumkin. Eslatib o'tamiz, moliyaviy piramidalarning asosiy maqsadi — uning yaratuvchisini yangi ishtirokchilar kiritgan mablag'lar hisobidan boyitishdir. Bunday piramidalarning aktivlari tashqi bozorda hech kimga kerak emas, ular foydalanishda hech qanday afzalliklarda ega emas, hech qanday muammoni ham hal qilmaydilar. Kriptovalyutalar bilan bog'liq holatda esa hammasi aksincha — ular moliyaviy bozorning katta muammosini hal qiladi, ularning aylanmasi qulay va ishtirokchilar uchun manfaatli bo'lib, bu ularni harid qilishga real talabni yuzaga keltiradi. Biroq ertaga bozor texnologik jihatdan yanada mukammal va qulay nimanidir ixtiro qilsa, yirik o'yinchilar va investorlar bitkoinga bo'lgan ishonchini yo'qotishi mumkin. Bu esa kursning tushib ketishi va kapitalning boshqa qulayroq vositaga o'tib ketishiga olib kelishi mumkin. Ammo hozirda bitkoinlar va boshqa kriptovalyutalarni mukammallashtirish ustida dunyo bo'ylab shunchalik ko'p iqtidorli programmistlar va matematiklar mehnat qilmoqdaki, navbatdagi keskin texnologik o'zgarish ehtimol mavjud texnologiyalar doirasida yuz berishi mumkin.

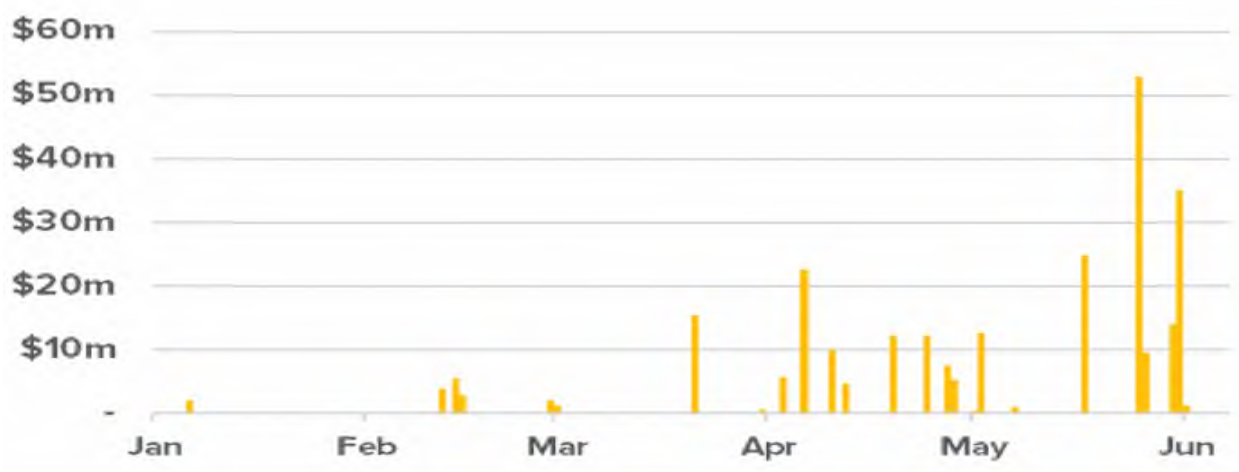
Bitkoin va boshqa kriptovalyutalar qiymati oshishining asosiy sababi bozorga yirik o'yinchilarning kirib kelishidadir. Investitsiya jamg'armalari, xalqaro korporatsiyalar, milliarderlar va hatto ba'zi davlatlar ham bir qator valyuta va texnologik blokcheynlarni qo'llab-quvvatlashi va foydalanishni boshlashi haqida



ma'lum qildi. Bu esa investorlar va kriptovalyuta sohiblarida ishonch uyg'otadi. Bitkoinni murakkab, ammo, real moliyaviy aktiv deb atash mumkin. **ICO** esa kriptovalyutalardan foydalangan xolda kompaniya tomonidan moliyaviy mablag' yig'ishning zamonaviy usulidir. Bu usul ko'proq birjada qimmatli qog'ozlarning joylashtirilishiga o'xshab ketadi. Bitkoin va efiriumlarning egalari esa kompaniyadan token deb atalmish boshqa turdagi kriptovalyutani oladilar. Tokenlarni esa **ICO** ga kirgan kompaniya maxsulotlariga almashtirish mumkin bo'ladi. **Runa Capital** venchur fondining mutaxassisi bildirishicha 2016 yili jahonda jami 150 ta **ICO** tashkil qilinib, ulardagi raqamli valyuta miqdori 500 million dollarga yetgan. Uning fikricha, davlat organlari **ICO** va raqamli valyutalar bilan bog'liq kontraktlarni tekshirish mexanizmini, kriptovalyuta foydalanuvchilarini aniqlash hamda ularning xuquqlarini himoya qilish va bu bilan bog'liq bo'lgan qonunlarni ishlab chiqishi zamon talabi bo'lib qolgan. Bu haqda batafsilroq quyidagi saytdan ma'lumot olishingiz mumkin:

<http://www.rbc.ru/finances/19/07/2017/596ecfc19a7947d191a18dc3?from=newsfeed>

ICO ga 2017 yilda jalb qilingan investitsiyalarni quyidagi diagramma orqali namoyish etishimiz mumkin (*mln dollarlarda*):



So'ming emissiyasi jarayonida blokcheyn texnologiyasini qo'llash orqali milliy kriptovalyutani yaratish ham O'zbekiston iqtisodiyotini rivojlantirishda muhim ahamiyatga molik bo'lishi mumkin. Chunki ushbu instrumentariy orqali O'zbekiston jahon kriptovalyutalar bozoriga kirib olib, iqtisodiyot rivojlanishi

AYUPOV R.H., KABULOV V.K.



uchun kerakli bo'lgan moliyaviy resurslarga ega bo'lishi mumkin. Shuni aytish mumkinki. 2013 yil noyabridan boshlab bitkoinning qiymati \$1000 dan oshdi, 2017 bahoriga kelib esa bitta virtual bitkoin uchun \$2500, kuziga kelib esa \$20000 bera boshlashdi. Ammo boshqa kriptovalyutalar ham o'sishda davom etmoqda. Masalan, bir Ethereum 2017 yil yanvaridan 2017 yil iyunigacha 30 barobar o'sdi va narxi \$250 ga yetdi. Bu o'sish bir qancha faktorlarga bog'liq. Masalan, 2017 yilda Yaponiya davlati xukumati bitkoinni to'lov vositasi sifatida tan olishdi va hozirda bu mamlakat fuqarolari ushbu kriptovalyutada bank hisob raqamlari ochishlari va undan foydalanishlari mumkin. Bitkoinning bu yetakchi rivojlangan mamlakatda qonuniylashtirilishi investorlar orasida katta qiziqish uyg'otmoqda, albatta. Masalan, 2017 yil may oyida ishga tushgan yapon kriptovalyuta birjasi **Z.com** talabgorlarning xaddan tashqari ko'pligidan ishini vaqtincha to'xtatib turishga majbur bo'ldi. Kriptovalyutalar narxining tezlik bilan oshib ketishi blokcheyn-ekotizimlarining rivojlanishi bilan ham bog'liqdir. Xususan, **ICO** mexanizmi (*blokcheyndagi kraudfunding*) tizimlari borgan sari ommalashib bormoqda. Startap kompaniyalar keyinchalik rivojlanish maqsadlarida o'zlarining shaxsiy kriptovalyutalarini ham chiqarishlari mumkin. Investorlar esa bu kriptovalyutalarni sotib olib, startap muvaffaqiyatli bo'lgan taqdirda yaxshigina foyda olishlari mumkin. Xozirgi kunlarda juda ko'p **ICO** lar tashkil etilmoqda va ular tomonidan jalb etilgan moliyaviy resurslar miqdori bo'yicha yangidan-yangi rekordlar qo'yilmoqda. Masalan, **Mozilla** brauzerining avvalgi bosh direktori Brendan tomonidan tashkil etilgan **Brave** startapi **ICO** vositasida 30 sekund davomida \$35 млн mablag' yig'a oldi. Nega bizning vatanimizda bunday texnologiyalarga qiziqish unchalik katta emas? Chunki, birinchidan, bizdagi bank-moliya mutaxassislari yangi texnologiyalarga juda extiyotkorlik bilan munosabatda bo'ladilar, ikkinchidan, ular tekshrilgan va uzoq muddat qo'llanilgan texnologiyalardan foydalanishi afzal ko'radilar va uchinchidan, bank-moliya sohasidagi mutaxassislarning amaliy va nazariy tayyorgarligi raqamli texnologiyalar nuqtai-nazaridan yetarli darajada emas. Ammo Kipr, Yaponiya, Rossiya, Xitoy, Singapur, Germaniya, Kanada va AQSh davrlari asta-sekin

AYUPOV R.H., KABULOV V.K.

raqamli electron valyutalarga o'tishni rejalashtirishmoqda. Masalan, 2016 yiling boshida Xitoy Xalq banki kriptovalyutaga o'tish rejasini e'lon qildi va hozirgi kunlarda naqd pullarni asta sekin blokcheynlarga o'tkazish uchun kerakli bo'lgan tadbirlar amalga oshirilmoqda. Xitoy mamlakati fuqarolari uchun bu ish hech qanday noqulaylik tug'dirmaydi, chunki bu tizimdan foydalanish hozirgi paytda foydalaniladigan **WeChat** yoki **Alipay** tizimlaridan unchalik farq qilmaydi. Ammo bu o'zgarish biznes uchun katta ahamiyatga ega bo'ladi, chunki bunda oradagi vositachilar yo'qoladi.

Uzbek milliy valyutasi – so'mni ham blokcheynga o'tkazish davlatga bir qancha muammolarni hal qilish imkonini berar edi. Shu jumladan:

- Joriy bank operatsiyalarining shaffofligini oshirish;
- Davlat sektori samaradorligini oshirish;
- Ikkilamchi va yashirin bank sektorini yo'q qilish;
- Davlat apparatidagi byurokrtiyani yengish;
- Soliqlar to'lash jarayonini mukammallashtirish orqali, soliq to'lamaslik xolatlariga qarshi samarador kurashish;
- Kichik biznes va tadbirkorlikning rivojlanishiga yangi imkoniyatlar berish;
- Halqaro valyuta-kredit resurslarini O'zbekiston iqtisodiyotiga keng jalb qilish;
- Moliya-kredit muassasalarining ishini yanada takomillashtirish va boshqalar.

Bunday xatti-harakatlarning muvaffaqiyatli ravishda rivojlanishi uchun mamlakatimizda to'rt xildagi yo'nalish taklif etish mumkin:

- Birinchi stsenariyda **bit so'm** muomalaga chiqarilishi mumkin. O'zbek milliy valyutasini blokcheynga va raqamli formatga o'tkazish unga bir qancha afzalliklar berishi mumkin, ammo bu holda bir qancha muammolarni qonunchilik asosida to'g'ri hal qilishga to'g'ri keladi. Masalan, ushbu blokcheynni kim boshqaradi va unga davlat maqomi beriladimi yoki u korporativ maqomga ega bo'ladimi. Bit so'm ichki va tashki bozorda qanday

ishlatiladi va kim tomonidan nazorat qilinadi degan savollarga ham konkret javob topish lozim bo'ladi.

- Ikkinchi yo'nalishda O'zbekistonda davlat blokcheyn tizimi tashkil qilinadi va u o'zida turli moliyaviy institutlarning funktsiyalarini qamrab oladi. Bunday institutlar jumlasiga banklar, depozitariylar, pensiya fondlari, soliq idoralari va boshqalarni kiritish mumkin. Bu amal soliq to'lash va mablag'larni fondlarga o'tkazish ishlarini avtomatlashtirish imkonini beradi.
- Uchinchi imkoniyat esa kriptovalyutani alohida tashkilotlarda yoki hududlarda hayotga tadbiq qilinadi va bu sohada yetarli tajriba to'planganidan so'ng bu ish respublika miqyosida amalga oshiriladi (*masalan, O'zbekiston Respublikasidagi ochiq iqtisodiy xududlarda yoki chet ellik mutaxassislar yordamida innovatsion korxonalarda*).
- Oxirgi, to'rtinchi imkoniyat esa Rossiydagidek Markaziy bank tomonidan raqamli kriptovalyutalar bilan ishlashni amalga oshiradigan pilot loyihani ishga tushirishdir (*mastercheyn loyihasi*). Ushbu platforma bozor ishtirokchilarining elektron usulda o'zaro ma'lumot almashinishi va blokchenlarda identifikatsiya qilinish uchun mo'ljallangandir. Bu tizim asta sekin, kriptop tajriba oshib borgan sari bir qancha davlat interaktiv xizmatlarining ham blokcheynga o'tkazilishini ta'minlashi mumkin.

Respublikamizda kriptovalyuta bo'yicha malakali mutaxassislarning juda kamligi va bu sohadagi tajriba ozligini hisobga olgan tarzda bu yo'nalishda malakali mutaxassislar tayyorlashni ham amalga oshirish zamona talabi bo'lib qolmoqda. Lekin blokcheyn texnologiyalarni hayotga tadbiq qilish va o'zbek kriptovalyutasini chiqarish innovatsion g'oyasini qadam ba qadam amalga oshirish hozirdanoq boshlab yo'lga qo'yilishi kerak bo'lgan hayot taqozosidir. Chunki dunyodagi ko'pchilik rivojlangan mamlakatlar o'zlarining milliy yoki korporativ kriptovalyuta loyihalarini amalga oshimoqdalar va ular keyinchalik barcha raqamli kriptopullarga egalik qilib, boshqa mamlakatlarni bu jarayondan siqib chiqarishga harakat qiladilar. Davlatning monetar siyosatidagi eng muhim amallardan biri pul emissiyasini nazorat qilish bo'lgani uchun, kriptovalyutadan voz kechish

AYUPOV R.H., KABULOV V.K.

mamlakatdagi moliya-kredit tizimini va uning jahon moliya kredit tizimi bilan aloqalarini sezilarli ravishda izdan chiqishiga olib kelishi mumkin.

### ***8. Kriptovalyutalarning investitsiyalardagi ahamiyati***

Endi kriptovalyutalarning investorlar uchun qanday qiyinchiliklar tug'dirishi masalasini ko'rib chiqamiz. Hozirgi davrda yangi raqamli texnologiyalar startap kompaniyalarga kriptovalyutalar yoki tokenlar ko'rinishida juda katta investitsion mablag'larni jalb qilish imkoniyatini yaratayapti. Misol uchun, yuqoridagi bo'limda ko'rsatilganidek, raqamli pullarni birlamchi joylashtirish – **ICO** (*initial coin offering*) o'nlab million pullarni investitsiyalar uchun to'plash imkonini yaratayapganini bir qancha davlatlardagi tajriba yaqqol namoish qilayapti. Ammo bu ishlarning manfiy oqibatlari ham vujudga kelishi ehtimoli bor albatta.



**ICO** vositasida investitsiyalar jalb qilinadigan startaplar bozorida yangi moliyaviy puffak paydo bo'lishi mumkin. Bunda emitentlar tomonidan hech qanday sarf-harajat qilinmagan xolda investorlar uchun yuqori darajada foyda olishlariga imkon yaratiladi. An'anaviy investitsion capital yig'ish usulida esa kompaniya kerakli kapitalni yig'a olish uchun uzoq yillar davomida aholining ishonchini qozongan bo'lishi kerak. Raqamli valyuta vositasida investitsion capital to'plash operatsiyasining qimmatli qog'ozlarni birlamchi aktsiyalar joylashtirish (*birjalarda sotish*) orqali amalga oshiriladigan an'anaviy usulidan asosiy farqi shundaki, bunda kompaniya sotuv uchun aktsiyalarni emas, balki tokenlarni (*raqamli jetonlarni*) chiqaradi. Buning uchun investorlar kriptovalyuta orqali to'lov qiladilar (*masalan, bitkoin yoki laytkoin orqali*). Mutaxassislarning fikricha, **ICO** emitentlari bu ishlarni qilayotganlariga katta tavakkalchiliklarga qo'l uradilar. Bu ayniqsa, kriptovalyutalar bozori faoliyati davlat boshqaruviga o'tgan paytda o'ta kuchayadi.

**ICO** tashkil qilish uchun kompaniya-emitent mahsus web-platformadan foydalanadi, masalan, **Waves** yoki **Ethereum** vositasiga qimmatli qog'ozlarning kriptoversiyasini chiqaradi. Buning uchun blokcheynga tranzaktsiyalar, ularning tavsifi, soni va unikal **ID** si bilan qo'shiladi. Emissiyadan so'ng tokenlarning istalgan sonligisini blokcheyndagi biror bir hamyondagi kriptovalyutaga almashish mumkin bo'ladi. Ba'zi bir kompaniyalar o'z tokenlarini oltin bilan yoki

kompaniyaning maxsuloti bilan ta'minlab beradilar. Masalan, **Ethereum** bazasidagi **DigixDAO** startapi 2016 yilda o'z tokenlarini oltin standartiga bog'lab chiqardi, amerikaning **Ethereum** asosida derivativlar bilan savdo qiladigan blokcheyn-platforma yaratayotgan **StabL** startapi esa o'z tokenlarini oddiy valyutada qiymati bo'lgan moliyaviy mahsulotlarga bog'lab qo'ydi. Tokenlarni chiqaradigan kompaniya-emitent va ularni sotib olishni istagan investorlar smart-kontrakt tuzishadi va buning asosida avtomatik blokcheyn-zanjirning ishtirokchilariga aylanadilar. Ushbu blokcheyn-zanjir doirasidagi kelishuvlar teskari kuchga ega emas. Token-kriptovalyuta oldi-sotti jarayoni quyidagicha tartibda amalga oshadi: Kompaniya dastur yordamida investorning hamyonini va investorga token jo'natiladigan hamyonni so'raydi. Kompaniya investordan kerakli summani olganidan so'ng, tranzaksiya amalga oshirigan hisoblanadi va smart-kontrakt ishga tushib, tokenlar xaridorga yetkazib beriladi. **ICO** tashkil qilgan kompaniya kryptoaksiyalarni (*tokenlarni*) bankka yoki venchur investorga emas, balki to'g'ridan-to'g'ri loyiha ishtirokchilariga sotadi. Demak, bu xolda loyiha ishtirokchilari kompaniya ishiga kuchliroq jalb qilinadilar, kompaniya mahsuloti va xizmatlaridan foydalanishga stimulyoladilar hamda boshqa insonlarga ham bu mahsulotlarni taklif qilish foydaliligini tushnadilar. Chunki, kompaniyaning ishi qanchalik yaxshi bo'lsa, investorlar ham shunchlik ko'p foyda oladilar.

Kriptoaksiyalarni birinchi bo'lib joylashtirgan kompaniya **Mastercoin** bo'lib, u 2013 yilda **ICO** yordamida \$500 ming dollar pul yig'a olgan. Blokcheyn texnologiyalar rivojlanishi bilan bu mablag' jalb qilish texnologiyasi yanada ko'proq qo'llanila boshlandi. **TechCrunch** ning ma'lum qilishicha, 2016 yilda umumiy summasi \$103 mln bo'lgan 64 **ICO** ishga tushirilgan. Keyingi davrlarda esa bir necha o'nlab kompaniyalar **ICO** tashkil qilinishi haqida xabar bermoqdalar, Shu jumladan, Rossiyaning **SONM** kompaniyasi kriptovalyutada \$42 mln jalb qilishga erishdi. **ICO** lar tarixidagi burilish nuqtasi bo'lib Kanadalik dasturchi Vitalik Buterinning **DAO** deb nomlangan loyihasini ko'rsatish mumkin. Bu loyiha doirasida kompaniya birdaniga \$152 mln investitsiya jalb qila oldi (*buni ko'pincha kraudfunding deb atashadi*). **DAO** loyihasi markazlashmagan venchur fond bo'lib, AYUPOV R.H., KABULOV V.K.

uning boshqaruvi dasturiy ta'minot vositasida avtomatik ravishda amalga oshiriladi. Ushbu xodisadan so'ng, jahon miqyosida **ICO** lar tashkil qilish jarayoni juda ham tezlashib ketdi. 2017 yil 30 may kuni JavaScript tili va Mozilla brauzeri ishlab chiqqan Brendan Ayk yangi Brave brauzeri ishlab chiqsh uchun **ICO** mexanizmi orqali \$35 mln yig'a oldi. Buning uchun Brendan **BAT** yoki **Basic Attention Token** deb nomlangan token yaratdi. Ushbu tokenlarning 1 milliarddan ortiqrog'i 156 000 **Ethereum** kriptovalyutasi birligiga sotildi (*ko'pincha bu valyutani efir deb ham atashadi*). Bu kriptovalyutaning bittasi narxi 2017 yil 23 iyun sanasiga \$327,42 deb baholandi.

**ICO** ga investor bo'lib an'anaviy moliyaviy instrumentlar bilan ishlash tajribasi yo'q insonlar ham qatnashishi mumkin. Shuning uchun ham tokenlarni ko'pincha malakali va professional investorlar emas, balki kriptovalyutaga ishonadigan yoki shu sohada ishlaydigan insonlar sotib olishadi. Bunday insonlar birjada yoki **Forex** da ishlash tajribalari yo'q bo'lgani bilan, ishni darhol kriptovalyuta biznesidan boshlaydilar. Kriptokraudfunding bilan bir qancha Rossiya kompaniyalari ham shug'ullanadilar va blokcheynlarni o'z loyihalari real iqtisodiyotiga tadbiq etadilar. Masalan, 2017 yil may oyida Moskva viloyatidagi "Kolionovo" nomli qishloq xo'jalik fermasi **ICO** yordamida \$500 ming jalb qilishga erishdi. Bu ferma "kolion" deb nomlangan mahsulot kuponlari chiqardi va uni fermaning mahsuloti bilan ta'minladi. Iyun oyida esa tsirkoniy ishlab chiqaradigan **ZrCoin** deb nomlangan Rossiya startap kompaniyasi **Waves** platformasidagi **ICO** vositasida 4000 investordan salkam \$7 mln investitsiya jalb qilishga erisha oldi. Bunda bir tokenning bahosi bir kilogram tsirkoniy dioksidi narxiga teng qilib olindi. Kompaniya jalb qilingan investitsiya yordamida zavod quradi va keynchalik o'z foydasidan investorlarga ularning tokenlariga mos ravishda to'lovlarni amalga oshiradi. Bu kompaniyalar kriptovalyuta tokenlarini real mahsulot ishlab chiqarishga bog'ladilar. Kompaniyalar blokcheynni o'z off-line bizneslarini rivojlantirish uchun qo'shimcha vosita sifatida ishlatdilar. Shuni ham aytish kerakki, **ICO** lar muvaffaqiyatining poydevorlaridan biri marketing jarayonini samarador va aqlga muvofiq ravishda amalga oshirishdir.

AYUPOV R.H., KABULOV V.K.

**ICO** bilan nafaqat startap kompaniyalar, balki yirik kompaniyalar ham qiziqqa boshlashayaptilar. 2017 yilda investorlar va startaplar uchun mo'ljallangan amerika platformasi taqsimlangan tarmoqlar qurish **Protocol Labs** kompaniyasi bilan hamkorlikda **CoinList** platformasini ishga tushirdilar. Bu platformaning missiyasi turli kompaniyalarga **ICO** tashkil qilishni osonlashtirishdir. Blokcheynlarni real biznesga tadbiq qilish imkoniyatlarini qidirishga bag'ishlangan va 2017 yil fevral oyida tashkil qilingan **Ethereum Enterprise Alliance** korxonalar al'yansiga xozirgi paytda 100 dan ortiq kompaniyalar kirgan. Bular jumlasiga **Microsoft, JPMorgan, Chase, Toyota, Merck** va boshqa katta kompaniyalarni kiritish mumkin. Shuning bilan bir qatorda bitkoinlarni to'lov vositasi sifatida qabul qiladigan yirik kompaniyalar soni ham ortib bormoqda. Misol sifatida quyidagilarni keltirishimiz mumkin:

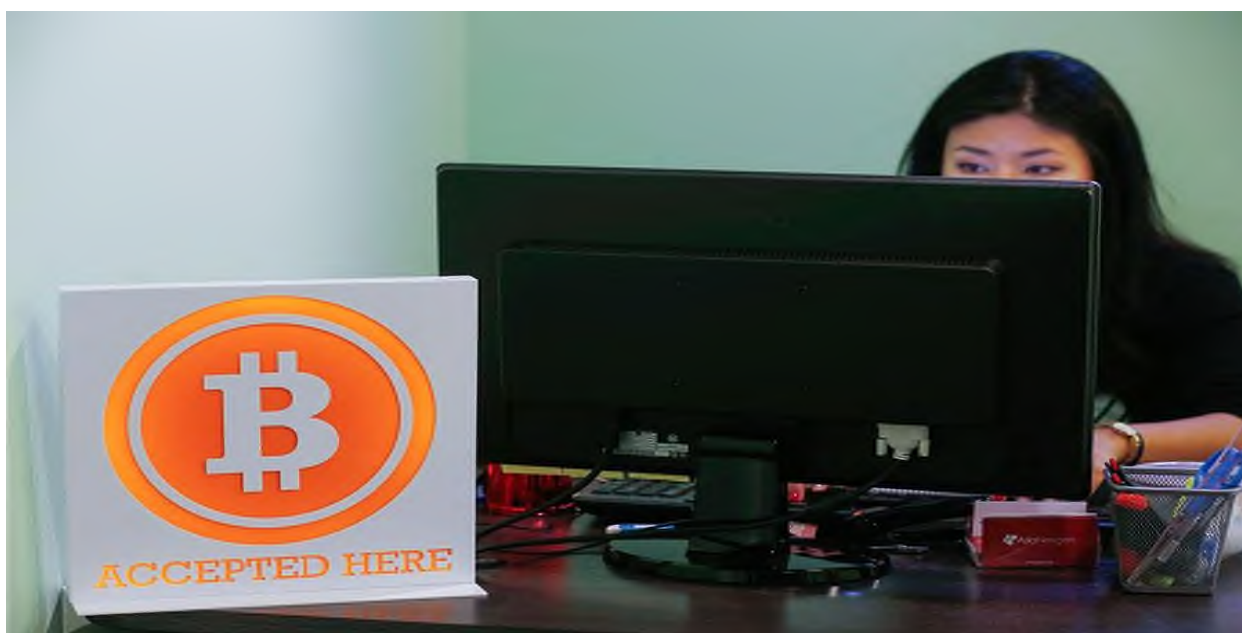
- ❖ Blog va saytlar yaratish platformasi **WordPress**
- ❖ Aviabiletlar qidirish sayti **Expedia**
- ❖ **PayPal** to'lov tizimi
- ❖ Yer yo'ldoshi televidenie provayderi **Dish Network**
- ❖ Latiya aviakompaniyasi **AirBaltic**
- ❖ Xaydovchilar chaqirish on-line servisi **Wheely**
- ❖ **Legal Prime GS Consulting** yuridik firmasi
- ❖ On-line supermarket **Yulmart**

Davlatlar tomonidan ham blokcheyn texnologiyalarga qiziqish ortgani bilan kriptovalyutalarning qonuniy jihatdan boshqariluvini yo'lga qo'yish jarayoni ancha past darajada. Masalan, Uzbekiston, Rossiya, Qozog'ston va boshqa hamdo'stlik mamlakatlarida kriptovalyutaning statusi umuman aniqlangan emas. Ularning konstitutsiyalarida kriptovalyutalarga o'xshash pul surrogatlarining pul aylanishida ishlatilishi qat'iyana ma'n etilgan. Ammo kriptovalyutalardan foydalanish asosida yotgan blokcheyn texnologiyasidan foydalanish ma'n etilgan emas. Lekin ba'zi mamlakatlarda nolegal tranzaksiyalarga qarshi kurash olib borish uchun kriptovalyutalardan foydalanish mumkinligi va uni qonuniylashtirish zarurligi bir qancha mamlakatlarda tan olingan. Agarda *“barcha qonuniy ravishda ma'n*

AYUPOV R.H., KABULOV V.K.



*etilmagan amallardan foydalanish mumkin*” degan mantiqiy qoidadan foydalansak, u xolda **ICO** ishtirokchilari qonunni buzmaydi deb o’zimizni ovuntirishimiz mumkin, albatta. Ammo tomonlar orasida tushumovchilik kelib chiqqanda, ularning o’z qonuniy xuquqlarini himoya qilishlari katta muammo bo’lib qolishi mumkin. Ya’ni tokenlarni kriptovalyutalarga sotib olish tomonlar orasidagi o’zaro kelishuvday bo’lib, o’zaro kelishmovchilik kelib chiqqan taqdirda shartnomani bajarmaslik uchun yetarlicha xuquqiy asos topish mumkin bo’ladi. Shuning uchun ham bizda xozircha kriptovalyutalardan faol foydalanishga shoshilmagan ma’qul.

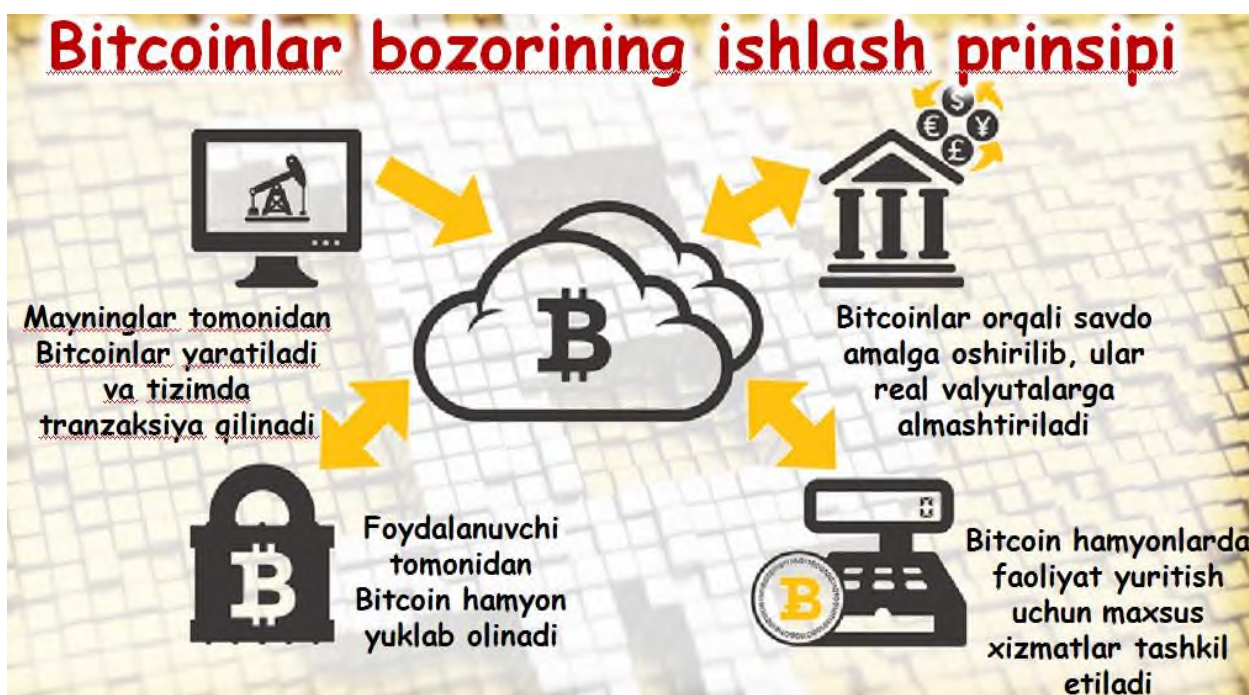


Keyingi paytlarda ko’plab kompaniyalar tomonidan **ICO** ga qiziqish tobora ortib borayotgani tufayli **Status** deb nomlangan Singapur blokcheyn-startapi tokenlarini joylashtirishda **Ethereum** platformasi ishida buzilishlar ro’y berdi. Kriptovalyutalarni o’rganishga bag’ishlangan ilmiy-izlanish **Smith + Crown** on-line resursi xozirgi vaqtda **ICO** tashkil qilayotgan yoki 2017 yil noyabrigacha bu ishni amalga oshirmoqchi bo’lgan 50 kompaniya haqida ma’lumot bergan. Buning ma’nosi shundaki, **ICO** lar atrofida moliyaviy puffak xosil bo’lmoqda va agarda bu puffak yorilsa, ushbu segmentgai investorlarning kriptovalyuta va tokenlarga bo’lgan qiziqishi sezilarli ravishda kamayishi mumkin. **ICO** larga bo’lgan katta qiziqish unchalik hayratlanarli emas, chunki **ICO** lar startup biznesga venchur investitsiyalarga nisbatan tezroq va qulayroq xolatda yaxshigina kapital jalb qilish

va tezda birjaga chiqishga imkon beradi. Haqiqatan ham klassik usulda investitsiyangizga capital jalb qilish uchun siz investorlar uchun taqdimot qilishingiz kerak, birjaga kelib, maslahatchilar yollashigiz lozim, aktsiyalar emissiya qilishingiz zarur, emissiya esa maxsus organlar tomonidan nazorat qilinadi va xakozo. Bu qiyinchiliklarni aylanib o'tib, investitsiyangiz uchun kerakli bo'lgan mablaglar'ni hozirda boshqarilmaydigan kriptovalyutalar bozoridan jalb qilish juda ham oson yo'l albatta. Lekin bu ishlarning xavfli tomonlari ham bor. Bu xududni *terra incognita* deb bilib, qonun bilan to'qnashib qolmaslik uchun extiyotkorlik bilan ish olib borish lozim bo'ladi. Istalgan xuquqiy yoki jismoniy shaxs, agar ularning ishonchini qozona olmasangiz, sizni *"kompaniya meni bu ish bilan bog'liq tavakkalchiliklar va risklar bilan to'liq tanishtirmagan"* deb, kompaniyani firibgarlikda ayblab, sudga berishi mumkin. *"Kriptovalyutalar yuqori darajadagi riskka ega bo'lgani uchun, xozircha ularga pul tikmagan ma'qul, chunki kompaniyaning sizga qandaydir daromad berishi ichun hech qanday huquqiy asos mavjud emas"* deb maslahat ham beradilar. Lekin ko'pchilik ekspertlarning fikriga ko'ra, uzoq muddatli perspektivada kriptovalyutalar bozori o'sishda davom etadi, blokcheyn texnologiyasi esa an'anaviy moliyada yanada kengroq miqyosda qo'llanilaveradi. Xozirda esa kriptovalyutalar olamida investorlar va kompaniyalar orasida hech qanday qonunchilikda ko'zda tutilgan xuquqiy asos bo'lmagani tufayli investorlarning juda katta miqdordagi daromad olishlariga imkon yaraladi hamda firibgarlik uchun ham katta imkoniyat paydo bo'ladi. Xozigi davrda ICO larda mayda investorlarni o'ng pullari aylanayapti, keyinchalik esa bu soxaga banklar, fondlar va davlat jalb qilinishi tufayli kriptovalyutaga qiziqish yanada ortadi. Xozircha kriptovalyutalar kursining bir oshib va bir kamayib turishi tabiiy xoldir. Kelajakda esa raqamli iqtisodiyotning rivojlanishi bilan, kriptovalyutalarga bo'lgan ehtiyoj tobora o'sib boraveradi va uning kursi ham yanada ortishi mumkin. Misol sifatida Rossiya birjalarining biri ham kriptovalyutalarni birja savdolariga qo'yish haqida tegishli ishlarni amalga oshirayotganini va Markaziy Bank tomonidan milliy kriptovalyutaning ishlatilishiga oid qonunlar ishlab chiqarilayotganini ko'rsatish mumkin.

## ***9. Kriptovalyutalar bozorida ishlash tamoillari***

Hozirgi paytda (2017 yil oxirida) kriptovalyutalar bozori hajmi \$82 milliard deb baholanadi. Izabella Kaminskaning ***Financial Times***dagi maqolasiga ko'ra, bu bozor optimizmga, ishonchga va va'dalar asosiga faoliyat ko'rsatadi. Raqamli pullarning nozikkina dunyosi yashirin bank tizimidan o'sib chiqib, asta-sekin puffakka aylanishi mumkin. Kriptovalyutalar bozoridagi xolatni u quyidagicha tavsif qiladi: *"Zimmasiga hech qanday majburiyatlar olmasdan millionlab dollar likvid moliyalashtirish evaziga istalgan kompaniya o'z shaxsiy valyutasini chiqara oladigan bozorni faraz qiling – buni men kriptovalyuta bozori degan bo'lar edim"*.



Uning fikricha, bu bozorda kompaniyalar biznesga uning xayotiyiligiga va potentsial foydaliligiga bog'liq bo'lmagan xolda pul jalb qilishga harakat qiladilar. Bu ishni qilishga ularni ambitsiyalari juda yuksakligi, ularda dasturiy kodning mavjudligi va o'z bizneslariga iloji boricha katta miqdordagi kapital jalb qilish istagi undaydi. Izabella Kaminskaning fikricha, hozirgi vaqtda kriptovalyutalar bozorida biror bir qiymatga ega bo'lmagan 900 dan ortiq kriptovalyutalar turi mavjud. Ularning eng mashhurlarini quyidagi jadvalda ko'rishimiz mumkin:

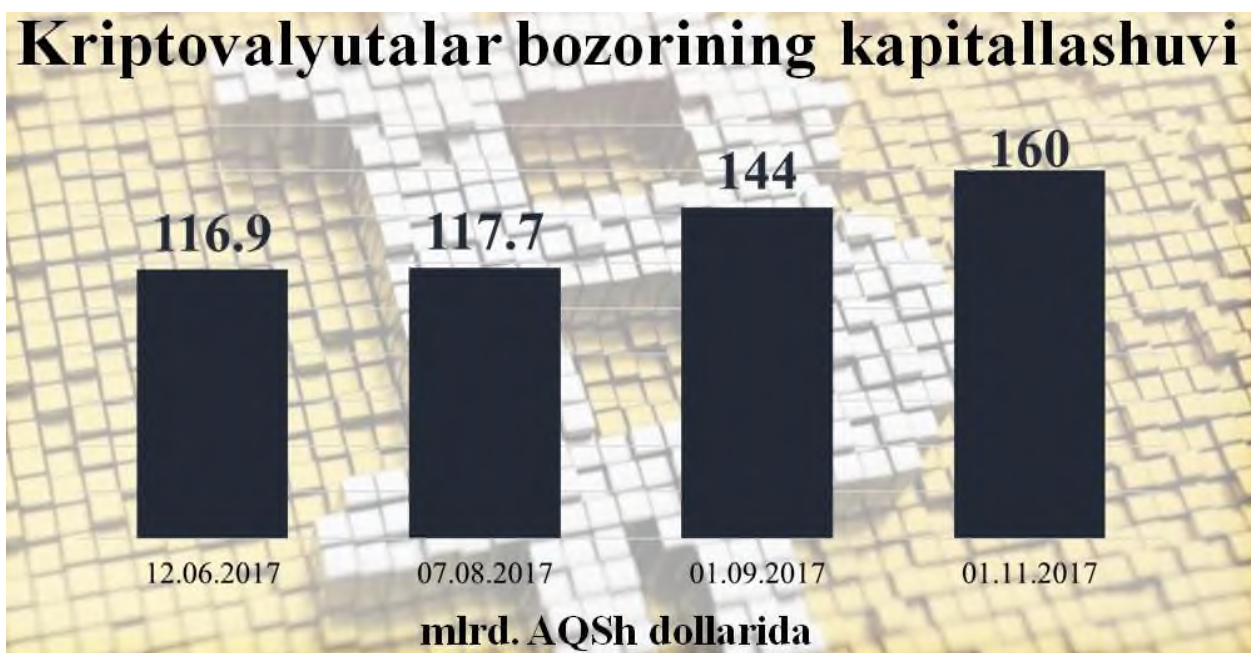
Nomi	Kodi	Paydo bo'lgan vaqti	Asoschisi	Bozor kapitali (2017-yil oktyabr holatida mln. AQSh dollari)
Bitcoin	BTC, XBT	2009	Satosi Nakamoto	89592
Ethereum	ETH	2015	Vitalik Buterin	28840
Ripple	XRP	2005/2011	Ripple Labs Inc.	8312
Bitcoin Cash	BCH	2017	Fork Block 8MB	5391
Litecoin	LTC	2011	Coblee	3067
Bitshares	BTS	2014	Daniel Larimer	140
Peercoin	PPC	2012	Sunny King	27
NXT	NXT	2013	BCNext	13
Namecoin	NMC	2011	Vinced	11

Masalan, 2017 yilning iyul oyida **EOS** kompaniyasi \$200 mln dollarlik kriptovalyuta jalb qildi, ammo uning tokenlari bozorda hech qanday ma'noga, funktsiyaga va imkoniyatga ega emas. Ba'zi startap kompaniyalar o'z faoliyatini

AYUPOV R.H., KABULOV V.K.

juda ham aniq va ravshan tavsiflamaydilar. Masalan, **InsureX** kompaniyasi o'z faoliyatini *“Blokchenlar asosidagi sug'urta qarorlarini qabul qilish”* deb tavsiflasa, **Pillar** kompaniyasi o'z faoliyatini *“Hamyonlarning ochiq kodli yangi avlodi”* deb tavsiflaydi. Shunga qaramay, ularga hech kim tokenlarni birlamchi joylashtirish (**ICO**) va an'anaviy venchur moliyalashtirish bilan solishtirila olinadigan miqdorda pullar jalb qilishlariga halal bermaydi. Bunda bir tomondan, **ICO** kompaniyalarga investitsiyalarni moliyalashtirishga imkon beradi, ikkinchi tomondan esa bu bozorning puffakka aylanish ehtimoli juda yuqori bo'ladi. Bu borada moliyaviy bozor expertlarining fikrlari turlicha va ba'zida bir-biriga qarama-qarshi. Masalan, **Deloitte** kompaniyasi va venchur investor Tim Dreyper **ICO** nexanizmi va kriptovalyutalarni qo'llab-quvvatlashadi. Ularning fikricha, vaqti kelib, kriptovalyuta bozori ishonchli bo'la boradi va **ICO** moliyalashtirishning juda yaxshi usuliga aylanadi. **Ethereum** ta'sischilaridan biri Charlz Xoskinson va uning hamfikrlari esa davlat boshqaruvi yoqligi tufayli vujudga keladigan risklar tufayli **ICO** ni asta-sekin portlaydigan bomba deb hisoblashadi. Iqtisodchi Izabella Kaminska ham kriptovalyutalar fenomenini yashirin bank tizimlari rivojlanishining navbatdagi evolyutsiya bosqichi deb atagan. Uning fikricha, oldingi davrlarda ham yashirin bank tizimlari xuddi shunga o'xshash to'lov vositasi statusini olgan pul vositalarini chiqarganlar. Moliyaviy inqiroz ro'y bergandan so'ng, davlat boshqaruvi asosida bunday to'lov vositalari yo'qolib ketgan va hozirda ular yana tokenlar va **ICO** lar ko'rinishida paydo bo'lganlar. Kriptovalyuta tokenlarini birlamchi joylashtirishda investorlar ushbu amal bo'yicha barcha risklarni o'z zimmlariga oladilar, kompaniya esa hech kimga hech nimani kafolatlamaydi. Ko'pchilik investorlar nimaga jalb qilinganliklarini va bu qanday oqibatlarga olib kelishi mumkinligini tushunmaydilar va davlat miqyosida yurisdiksiyaning yo'qligi ularga katta tosiq bo'lib qoladi. Xuddi shuning uchun ham bir qancha mamlakatlarda kriptopullarning va tokenlarning birlamchi joylashtirish jarayonini qonuniy asosga qo'yish ishlari olib borilmoqda.





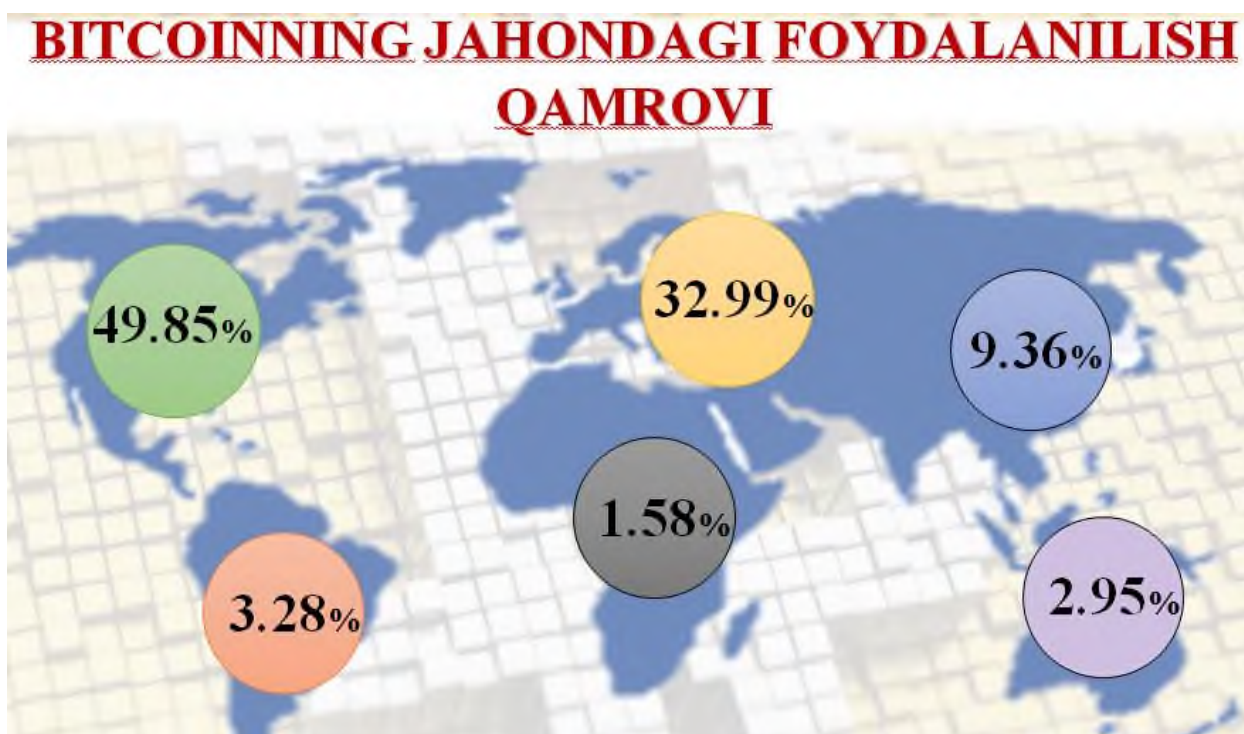
Reuters agentligining bildirishicha, **Linux Foundation** boshchilik qiladigan **Hyperledger** blokcheyn-konsortsiumi katta biznes uchun o'z blokcheynlaridan foydalana oladigan ilk taqsimlangan reestrning dasturiy kodini chiqardi. Bu loyiha jahondagi bir qancha yirik kompaniyalarni birlashtiradi, shu jumladan, **IBM**, **Cisco**, **JPMorgan Chase & Co**, **Sberbank** va boshqalar. **Hyperledger Fabric 1.0**. deb atalgan ushbu taqsimlangan reestr – blokcheyn havfsiz va ishonchli bo'lib, katta kompaniyalar uni o'z biznes jarayonlariga bimalol ishlatishlari mumkin. Bu blokcheyndan foydalanish banklarga va moliyaviy tashkilotlarga eng murakkab jarayonlarni, masalan, qimmatli qog'ozlar bo'yicha operatsiyalarni boshqarishni osonlashtirishga imkon beradi. Ushbu ishlarni amalga oshirish texnologiyalarini ishlab chiqish uchun kompaniyalar millionlab dollar investitsiya qiladilar. Bu ishlarni tezlashtirish uchun katta kompaniyalar tarmoq guruhlari tashkil etadilar. **Hyperledger** huddi shunday guruhlarining biri va u sof texnik tashkilot deb tushuniladi. **JPMorgan**, **Microsoft** va **Intel** kompaniyalari **Ethereum Enterprise** al'yansiga kirdilar. Blokcheyn juda katta moliyaviy kompaniyalarni o'ziga jalb qila oldi. Ammo, shuni ham aytish kerakki, **Hyperledger Fabric 1.0** xozircha katta an'anaviy to'lov tizimlari amalga oshiradigan darajadagi tranzaksiyalarni eplay olmaydi, ammo, **Hyperledger** mutaxassislarining fikricha, tizimning quvvati tez orada ancha miqdorga oshiriladi

va u real biznes uchun juda ham mos xolatga keladi. 2017 yilning 1 avgustidan boshlab bitkoin ikkita valyuta turiga bo'lindi – **Bitcoin (BTC)** va **BitcoinCash (BCH)**. **BTC** ning o'sha paytdagi kursi 4020,22 ming dollar, **BCH** ning kursi esa 299,36 dollar edi. **BTC** ning o'sha davrdagi kapitalizatsiyasi 66,348 milliard dollar bo'lgan bo'lsa, **Ethereum** ning kapitalizatsiyasi 28 milliard dollar, narxi esa 299,23 dollar bo'lgan. Uchinchi o'rinda **Ripple** deb nomlangan kriptovalyuta turadi. Uning kapitalizatsiyasi 6,3 milliard dollar bo'lib, narxi 0,17 dollar.



Qo'shni davlat Qozog'istonda ham iqtisodiyotni keskin modernizatsiyalash yo'liga o'tib, "**Raqamli Gozog'iston**" davlat dasturi ishlab chiqildi va u amalga oshirilmoqda. Shuni ham ta'kidlash kerakki, Qozog'ston jahon miqyosida davlat darajasida kriptovalyuta tizimini rivojlantirish zarurligini tan olgan Yaponiya davlatidan keyingi ikkinchi davlat hisoblanadi. Blokcheyn-texnologiyalarni o'rganish maqsadida "**Ostona**" Xalqaro moliyaviy markazi qoshida taniqli kompaniyalar ishtirokida ishchi guruh tuzilgan. Mutaxassislarning fikricha, 2018-2019 yillarda Qozog'ston blokcheyn texnologiyalarni moliyaviy va davlat sektorida qo'llash uchun imkoniyatlar yaratadi. "*Raqamli Gozog'iston*" davlat dasturi hamda moliyaviy markaz ishchi guruhi mamlakatda blokcheyn

texnologiyalarni qo'llash jarayonini boshlab yuboradi. Shuning uchun ham bitkoin va blokcheynlarga bag'ishlangan konferentsiyalar o'tkazish bo'yicha yetakchi **Smile-Expo** kompaniyasi shunday tadbirni Qoz'g'stonning Almati shaxrida o'tkazishga qaror qildi. **Blockchain & Bitcoin Conference – Rossiya, Angliya, Mal'ta, Chexiya, Litva va Ukrainada** o'tkasilayotgan kriptovalyutalar taraqqiyotiga bag'ishlangan tadbirlar kompleksidir. Ushbu tadbirlar davomida keyingi to'rt yilda blokcheyn texnologiyalar mutazassislari, kriptovalyuta bozori ishtirokchilarini va **ICO** ni ishga tushirish bo'yicha nutaxassislarni birlashtirib, ularning malakasini ancha oshirishga erishildi. **Blockchain & Bitcoin Conference Almaty 2017** anjumanida ham moliyaviy texnologiyalar soxasidagi yangiliklarni biznes va davlat organlarida qanday ishlatilishi mumkinligi masalalari muxokama etildi. Shu bilan birga, kraudfundingning (**ICO**) dolzarb muammolari hamda innovatsion moliyaviy texnologiyalarning davlat tomonidan boshqariluv masalalari ham o'rganib chiqildi.



Rossiyalik bir qancha moliyaviy analitiklarning fikrlariga ko'ra, kriptovalyutalarni amalga kiritilishi va ularni bir qancha mamlakatlarda to'lov vositasi sifatida ishlatilina boshlashi jahon moliyaviy tizimi uchun ilk marotaba 70 yil davom etgan AQSH valyuta gegemoniyasidan qutulish uchun bir imkoniyatdir,



chunki AQSH davlati o'z vaqtida butun dunyo uchun o'z milliy valyutasini rezerv valyuta sifatida ishlatishning uddasidan chiqdi va shu sababli ham pul stanoklarida doimiy ravishda dollar chop qilgan xolda barcha mamlakatlardagi moliyaviy aktivlarni sotib ola boshladilar va hozir ham faol sotib olmoqdalar. Bundan qutulish va mamlakat moliyaviy mustaqilligini ta'minlash uchun qandaydir yangi valyutani ishlab chiqish va tan olinishining qonuniy yo'l-yo'riqlarini ishlab chiqish O'zbekiston iqtisodiyoti uchun ijobiy amallardan biri bo'lgan bo'lar edi.

Quyida jahondagi turli mamlakatlar miqyosida kriptovalyutalar bilan ishlash imkoniyatlari grafik tarzda keltirilgan:





### *Litsenziya bilan tartibga solinadi*

- Tovar sifatida tan olingan
- To'lov vositasi sifatida tan olingan



### *Qonunan taqiqlanmagan*

- Savdo obyekti sifatida tan olingan
- To'lov vositasi sifatida qabul qilinmagan



### *Foydalanish qonunan taqiqlangan*

- 2017-yil sentabrga qadar muomalada bo'lgan



### *Taqiqlanmagan*

- To'lov vositasi sifatida tan olingan
- Shaxsiy mulk sifatida qaraladi



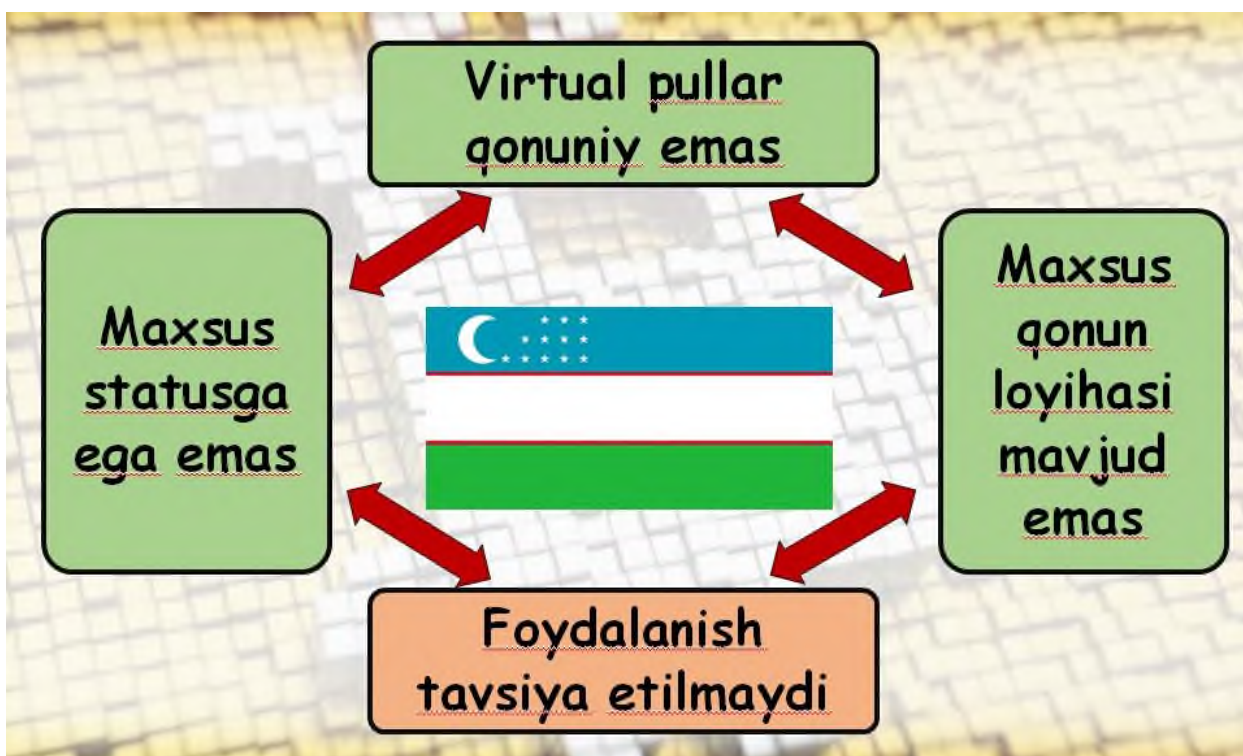
### *Taqiqlanmagan*

- To'lov vositasi sifatida tan olingan
- Ulardan olingan daromad soliqqa tortiladi



### *Taqiqlanmagan*

- To'lov vositasi sifatida tan olingan
- Ulardan olingan daromad soliqqa tortiladi



Endi hozirgi davrdagi eng ahamiyatli besh kriptovalyuta va uning xususiyatlari haqida yuqorida aytilgalarga qo'shimcha bo'lgan ma'lumotlarni keltiramiz.

### ***Bitcoin***

Xozirgi vaqtda kriptovalyutalarning ichida eng keng tarqalgani bitcoin hisoblanadi. Uning protokoli Satoshi Nakamoto ismli inson boshchilik qiladigan guruh tomonidan ishlab chiqilgan deyiladi. 2008 yilda Nakamoto muallifligida *Bitcoin: A Peer-to-Peer Electronic Cash System*, deb nomlangan maqola chop etilib, unda tamoman markazlashmagan va uchinchi tomonlarning ishonchini talab qilmaydigan elektron naqd pullar tizimi qanday faoliyat ko'rsatishi tavsif etilgan.





www.coindesk.com

Ammo, 2016 yilning may oyida avstraliyalik Kreyg Rayt ham bitkoin tizimini men ishlab chiqqanman deb da'vo qilgan. Xozirgi paytda (2017 yil yoz oylari) bitkoinning bozoriy kapitalizatsiyasi 44,6 milliard dollar atrofida deb ko'rsatiladi bir qancha manba'larda.

### *«Ethereum yoki Efir»*



www.coindesk.com

Bu kriptovalyuta bozori xozirgi paytdagi (2017 yil) kapitalizatsiyasi bo'yicha ikkinchi o'rinda turib, ushbu ko'rsatgich unda 21 milliard dollar atrofida deb aytiladi. Bu kriptovalyuta Kanadalik dasturchi Vitalik Buterin loyihasining kraudfanding usulidagi moliyalashtirish uchun yaratilgan edi. **Ethereum** o'ziga o'rnatilgan dasturiy tilga ega bo'lgan ochiq platforma bo'lib, uning asosiy g'oyasi istalgan dasturchiga **blokcheyn** texnologiya asosida qo'shimcha amaliy dasturlar ishlab chiqish imkoniyatini yaratishdir. Ushbu kriptovalyutaning chiqarilish

AYUPOV R.H., KABULOV V.K.





[www.coindesk.com](http://www.coindesk.com)

Bozoriy kapitalizatsiya bo'yicha to'rtinchi o'rinni **Ripple** kriptovalyutasi egallaydi. Bu valyutaning protokoli tomonlar orasidagi pul o'tkazmalarini istalgan ko'rinishda va bevosita amalga oshiradi hamda buning uchun komissiya miqdori minimal miqdorda o'rnatilgan. **Ripple** tizimi 2012 yilda ishga tushirilgan va tezda moliyaviy institutlar va banklarning diqqat-e'tiborini o'ziga tortgan. 2017 yilning aprel oyiga bo'lgan ma'lumotlarga ko'ra Ripple mijozlari ichida 75 ta bank bor ekan, shu jumladan, **BBVA**, **StandardChartered** va **Bank of America**. Ripple ning hozirgi paytdagi kapitalizatsiyasi 6,7 milliard dollarni tashkil qiladi.

## Litecoin





[www.coindesk.com](http://www.coindesk.com)

Bozoriy kapitalizatsiya bo'yicha beshinchi o'rinda turadigan kriptovalyutaga **Litecoin** kiradi. Bu raqamli valyuta turi 2011 yil oktyabr oyida bitkoinning bir turi (*forki*) sifatida dunyo yuzini ko'rdi. Uning asoschisi oldingi davrda **Google** da ishlagan dasturchi Charli Lee edi. Ushbu kriptovalyutaning saytida aytilishicha, bu valyuta tranzaksiyalarning tasdiqlanishi tezligi va bitkoinga nisbatan saqlanish samaradorligi kattaligi bilan boshqalaridan farq qiladi. Undan tashqari, **Litekoin** tarmoq quvvatlanuvi mavjudligi, savdo aylanmasi va likvidliligi bilan farqlanadi hamda bitkoinga qo'shimcha ravishda electron tijorat uchun tekshiruvdan o'tgan vosita deb uqtiriladi. Hozirgi paytda Laytkoinning umumiy kapitalizatsiyasi 2,2 milliard dollardan yuqori.

Endi esa O'zbekistonda kriptovalyutadan foydalangan xolda qanday qilib biznesni amalga oshirish mumkin, qanday qilib kriptovalyutalarga investitsiya qilish mumkin, qanday kriptovalyutani tanlash lozim, qanday qilib ishonchga sazovor birjani topish va unda qanday qilib registratsiya qilinish masalalari bo'yicha "**Alpari**" kompaniyasining mutaxassislari fikrlari bilan tanishib chiqamiz.



Kriptovalyutalar kursining tezlik bilan o'sishi investorlar tomonidan juda katta qiziqish uyg'otmoqda. Dunyoda eng ommaviy bo'lishga ulgurgan bitkoin kriptovalyutasi 2017 yil boshidan buyon salkan 400% ga o'sdi, laytkoin va efiriumlarning narxlari esa yil davomida 10 barobarga o'sdi. Daromadning bu darajada katta miqdorda o'sishini hech qanday bank yoki investitsion fond ta'minlab bera olmaydi. Shuning uchun ham, qanday qilib kriptovalyutalarga investitsiya qilish mumkin va qanday kriptovalyutalani tanlash maqsadga muvofiq bo'ladi degan savolga javob topish investorlar uchun juda muhim hisoblanadi. Chunki kriptovalyutalar bozori bir qancha o'ziga xos jihatlarga va tushunarsiz xolatlarga ega. Eng avval kriptovalyuta sotib olish uchun birjani tanlash kerak bo'ladi, birjaning ishonchlilik darajasini chamalash va unda registratsiya qilingandan so'ng, kriptovalyutani qaerda saqlash masalasini hal qilish lozim bo'ladi. Buning uchun esa kriptohamyon (*koshelek, wallet*) lardan birini tanlash va unda qayd qilinish talab etiladi. Bu ishlarni amalga oshirish anchagina mehnat va vaqt talab qiladi alatta. Ammo agarda sizda kriptovalyutalar bozorida faoliyat ko'rsatish bo'yicha kerakli bolgan bu ishlarni qilishga vaqt va ishtiyoq bo'lmasa, ammo uning investitsion potentsialidan foydalanib, bir oz mablag' ishlab olishni

ALIFOV R.H., KADLOV V.R.



istasangiz, u xolda siz tomoningizdan qabul qilinishi mumkin bo'lgan eng yaxshi yechimlardan biri – eng perspektiv kriptovalyutalarni o'z tarkibiga qamrab olgan tayyor investitsion portfel sotib olishdir. Bunday tayyor mahsulotlardan biri xalqaro moliya tashkiloti **Alpari** tomonidan ishlab chiqilgan va bozorga taqdim etilgan **CryptA Capital** investitsion portfelidir. Ushbu investitsion portfel investitsiya qilish oddiyligi va yaxshi daromadni ta'minlashi bo'yicha O'zbekistonlik xususiy investorlar orasida talabgor hisoblanadi.



**CryptA Capital** investitsion portfeli orqali kriptovalyutalar bozoriga qilingan investitsiyalardan foydani uch asosiy ommabop kriptovalyutalar – bitkoin, laytkoin va efirium orqali olish mumkin bo'ladi. Jahon bozorida bu kriptovalyutalarga bo'lgan talabning juda yuqoriligi ular asosida yaratilgan investitsion portfelning katta samaradorligiga olib keladi. Demak, **CryptA Capital** investitsion portfelining eng asosiy afzalligi, uning diversifikatsiyasi, ya'ni, unda birdaniga uchta valyutaga investitsiya amalga oshirilgan. **Alpari** kriptoportfelining yana bir afzalligi unga investitsiya qilishning oddiligidir. Buning uchun portfelning barchasini sotib olish talab qilinmaydi, uning token deb atalmish bir qismini sotib olish kifoya. Shundan so'ng, "*Shaxsiy cabinet*" dagi daromadlar dinamikasi statistikasini kuzatib turish kerak bo'ladi xolos. **CryptA Capital** investitsion portfeliga bir yil muddat bilan investitsiya kiritish mumkin, ammo investor undan

muddatidan avval chiqmoqchi bo'lsa, u xolda o'z tokenlarini sotish orqali, investitsion portfeldan chiqib ketish mumkin bo'ladi.

Kriptovalyutalar bozoriga investitsiyalar boshqa an'anaviy bozorlarga bo'lgan investitsiyalarga nisbatan ancha katta daromad berishi bilan farqlanadi. Masalan, token narxlarining 500 dan 1000 birlikkacha o'sishi investor uchun 100% daromad kelganini anglatadi. Shuning uchun investitsion portfeldagi tokenlarni o'z vaqtida sotib olish va kerakli paytda qayta sotish ahamiyatli hisoblanadi. Tokenlar narxi hozirgi paytda qancha ekanligini bilish uchun esa **Alpari** saytining tegishli bo'limiga nazar solish kifoya. Raqamli valyutalarga bo'lgan qiziqishning ortib borishi ertami-kech bu moliyaviy aktivlarning yetishmovchiligiga olib keladi va ularning narxi yanada oshaveradi. Xuddi shu sababli ham kriptovalyutalar portfeli eng perspektiv investitsion mexanizm hisoblanadi. Hozirgi paytda **CryptA Capital** investitsion portfeliga kirish narxi 100 dollar turadi, ammo moliyaviy analitiklarning fikrlaricha, investitsiyadan kattaroq daromad olish uchun 1000 dollardan ko'proq investitsiya qilgan ma'qul. Agarda siz kriptovalyutalar vositasida kattaroq daromad olishni istasangiz, **CryptA Capital** investitsion portfeliga yoki shunga o'xshash investitsion portfellardan biriga diqqatingizni qaratishingiz foydadan xoli bo'lmaydi. Bu haqda **alpari.com** saytiga murojaat qilishingiz va kerakli ma'lumotlarni bilib olishingiz mumkin.

**Belorusiya** prezidenti tomonidan imzo qo'yilgan *“Raqamli iqtisodiyotni rivojlantirish”* dekreti bu mamlakatda raqami valyutalar va tokenlarni legalizatsiya qiladi. Unda aytilishicha *“Huquqiy shaxslar “Yuqori texnologiyalar parki” rezidentlari bilan birgalikda o'z tokenlariga ega bo'lishlari, tokenlarni chiqarishlari va joylashtirishlari, sotishlari va boshqa operatsiyalarni amalga oshirishlari mumkin. Ammo bu ishni ular faqatgina kriptovalyuta birjalari hamda kriptovalyuta almashinuv operatorlari orqali amalga oshira oladilar”*. Jismoniy shaxslarda ham tokenlar bo'yicha operatsiyalarni amalga oshirish va ularga egalik qilish huquqi bo'ladi. *“Jismoniy shaxslarning mayning bo'yicha, tokenlarni sotib olish va ularni sotish bo'yicha faoliyatlari tadbirkorlik faoliyati deb hisoblanmaydi va tokenlar hamda ulardan olingan daromadlar deklaratsiya qilinmaydi”*.

Kriptovalyutalardan olinadigan daromadlardan esa 2023 yil 01 yanvargacha soliq to'lanmaydi. Belorussiya mutasaddilari kriptovalyutalar bozorini rivojlantirish orqali mamlakatga real investitsiyalar oqimini (*ya'ni, kriptovalyutalar orqali real pullarni*) ko'paytirishni reja qilishgan chog'i. Ammo, nima bo'lganida ham bu dekret Beloresiyada **IT**-sohaning tezlik bilan rivojlanishiga olib kelishi aniq.

Bo'lim oxirida shuni ham aytishimizkerakki, hosirgi davrga kelib, **iPhone** larning egalari ham **MobileMiner** dasturi yordamida bitkoinlarni mayning qilishlari mumkin. Bu bo'yicha qo'shimcha ma'lumotlarni quyidagi saytdan bilib olishingiz mumkin: [https://rueconomics.ru/297707-vladelcy-iphone-smogut-dobyvat-bitkoiny-s-pomoshchyu-prilozheniya-mobileminer#from\\_copy](https://rueconomics.ru/297707-vladelcy-iphone-smogut-dobyvat-bitkoiny-s-pomoshchyu-prilozheniya-mobileminer#from_copy)

## **10. Kriptovalyuta birjalarida ishlash**

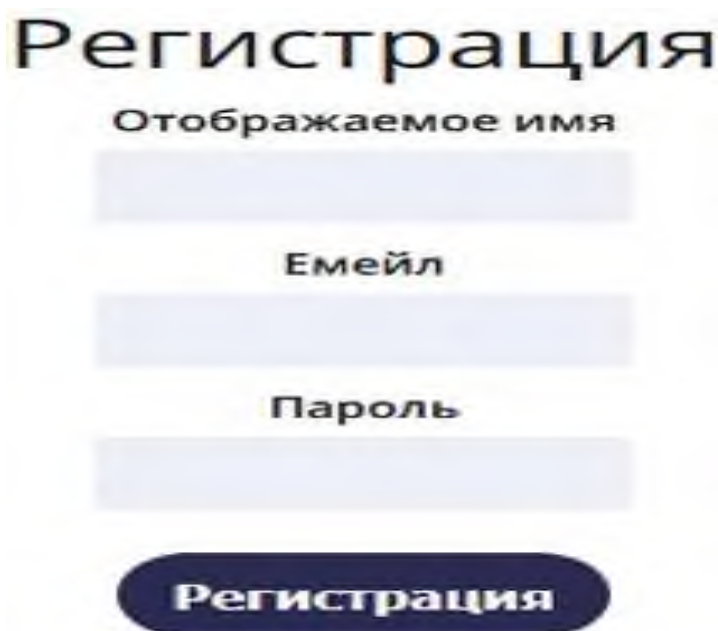
Ushbu bo'limda kriptovalyutalar bo'yicha real operatsiyalarini mustaqil ravishda amalga oshirish mumkin bo'lgan bir qancha birjalar va ularning almashinuv punktlari bilan tanishib chiqamiz hamda bo'lim oxirida kriptovalyutalar bozorida ishlashni boshlash uchun zarur bo'lgan eng muhim masalani – ularni qanday qilib sotib olish mumkinligini batafsil ko'rib chiqamiz. **Mitsubishi UFJ Financial Group** banki ham o'z kriptovalyuta birjasini hamda milliy valyutaga bog'liq bo'lgan tokenlarni ishga tushirishni rejalashtirayapti. Alohida bitkoin akkauntlarni boshqaruvchi servis tashkil qilish ham ko'zda tutilayapti.



Ushbu bank bu ishni 2018 yilda amalga oshirmoqchi va moliyaviy xizmatlar bo'yicha agentlik **FSA** bu ishni ko'rib chiqmoqda. Bu kriptovalyutaning nomi bank abbreviaturasidan kelib chiqqan xolda **MUFG Coin** deb nomlanar ekan. Ishonchlilikni ta'minlash uchun bu kriptovalyuta yapon tangasi bilan 1:1 nisbatda bo'ladi va keyinchalik kursi o'zgarishi mumkin bo'ladi. Bunday qilishdan maqsad, narxlar tez-tez o'zgarishining oldini olish va foydalanuvchilarning ishonchini qozonishdir. Bankdan olingan ma'lumotlarga ko'ra, u kriptovalyuta treyderlari uchun shahsiy servis tashkil qilish ustida ham ishlayapti. Shu servis tufayli savdolarni tashqi birjalarsiz amalga oshirish mumkin bo'ladi va natijada barcha valyuta bank ihtiyorida qoladi. Shunday qilib, bank har qanday xolatda ham mijozlarning mablag'lari havfsizligini ta'minlab beradi. Servis har bir akkaunddagi ko'zda tutilmagan faolliklarni tahlil qilib, ularning himoyasini qattiq nazorat qiladi.

Yana bir kriptovalyuta birjasi **Bitflip (BitFlip)** deb nomlanadi va unda bitkoinlarni webmaniga sotib olish mumkin. Quyida ushbu birjada qanday qilib ishlash amaliyoti tavsif etiladi.

1. **Bitflip** birjasida registratsiya qilinish uchun 3 ta maydonni to'ldirish kerak bo'ladi: foydalanuvchi nomi, electron pochtasi va paroli. Shundan so'ng "**Registratsiya**" tugmachasi bosiladi. Shundan so'nggina o'z akkauntingizga kirasiz. Quyida o'sha maydonlar aks ettirilgan:



Регистрация

Отображаемое имя

Емейл

Пароль

Регистрация

2. Bitflipda hisob raqamini to'ldirish uchun asosiy sahifaning o'ng yuqori burchagidagi *“Moi koshelki”* deb nomlangan tugmachani turtish kerak. Shundan so'ng ekranda bir qancha hamyonlardan iborat sahifa ochiladi. Bulardan to'rttasi USD, EUR, RUB va YAN valyuta hamyonlari bo'lib, 15 tasi esa kriptovalyutalar hamyonlaridir (BTC (bitkoin), THB, LTC (laytkoin), ETH (efirium), XRP (ripple), DASH (dash), DOGE, BCH (bitcash), FLIP, R, RMC, BTG, XRB (reybloks), TRX (tron), FOOD).
3. **Bitflip** birjasida webmaniga, dollarga, evroga va rublga kriptovalyuta sotib olish mumkin.

**Binance** birjasi ham zamonaviy kriptovalyuta savdo maydoni hisoblanadi va u orqali foydalanuvchilar qulay va havfsiz ravishda raqamli valyutalar sotib olishlari va ularni boshqalariga almashtirishlari mumkin.



Shanxayda joylashgan bu birja 2017 yilda ishga tushgan bo'lib, juda ko'p miqdordagi mijozlarga ega va ancha ommabop hisoblanadi. Savdo hajmi bo'yicha bu birja top 14 ta birjalardan biri hisoblanadi. Uning yana bir asosiy faoliyat doiralaridan biri blokcheyn aktivlaridir. Birjani ilgari **OKCoin**, **Blockchain.info** va **Bloomberg** kompaniyalarida yuqori mansablarda ishlagan inson Chjao boshqaradi. Hozirgi kunda **Binance** birjasi savdo oboroti bo'yicha dunyoda beshinchi o'rinni egallaydi (*sutkasiga 0,6 milliard dollar*).

Birjada akkaunt hosil qilish uchun saytga kirish va registratsiya formasini ochib, unga emailni, parolni va kaptni (*tasvirli simvollarni*) ikki bosqichda kiritish kerak bo'ladi. Ko'rsatilgan pochta qutisini tasdiqlash uchun unga yuborilgan xatdagi ilovaga o'tiladi. Shu xarakatlardan so'ng, akkaunt hosil bo'ladi va shundan keyin avtorizatsiyaga o'tish mumkin bo'ladi. Verifikatsiya qilish

jarayoni uch qadamdan iborat bo'ladi. Birinchi qadamda emailni tasdiqlashda o'tasiz va endi tizimdan kuniga 2 bitkoinidan ortig'ini chiqara olmaysiz. Ikkinchi qadamda *“shaxsni tekshirishni tugallash”* bo'limini turtish kerak bo'ladi. Buning uchun esa telefon raqamini tasdiqlash lozim bo'ladi. Buni amalga oshirish uchun bir qancha xujjatlar talab qilinadi. Agarda bu qadamni tugallasangiz, endi tizimdan kuniga 100 tagacha bitkoin chiqara olasiz. Agarda uchinchi qadamni ham amalga oshirish kerak bo'lib qolsa, u xolda texnik yordam hizmatiga murojaat qilish kerak bo'ladi. **Binance** da fiat vositalar bilan hisob raqamini to'ldirish ko'zda tutilmagan. Hisobni to'ldirish uchun eng oldin Bitkoin yoki Efir sotib olish lozim. Shundan so'ng sotib olingan kriptovalyutangizni Binance dagi hisob raqamiga kiritasiz. Hisob raqamini to'ldirish uchun kursorni **“aktiv”**ga keltirib, so'ngra **“Balans”** tugmachasi bosiladi. Shundan so'ng siz ishlay olish mumkin bo'lgan valyutalarni ko'rasiz va **“Depozit”** tugmachasini turtib, kerakli vositani kiritishingiz mumkin. Xozirgi kunga 44 valyuta bilan ishlay olish mumkin. Savdoni amalga oshirish uchun **“Savdo markazi”** ga o'tiladi va undagi savdo juftlari tanlanganida grafik va order savatchasi paydo bo'ladi. Agarda bu yerdan kerakli juftlikni topa olmasangiz, u xolda **More** tugmachasini bosib, ruyhatdan keraklisini tanlab olasiz. Hozirgi kunda orderlarning ikki variant **Limit** va **Market** dan foydalanish mumkin. Agarda birinchi variantni tanlasangiz, boshlang'ich narxni va kriptovalyutalar sonini aniqlab, sotuv yoki xarid tugmachasini bosasiz. Birja komissiyasi savdo hajmining 0,1% ni tashkil qiladi.

**HitBTC** birjasi olti million dollar boshlang'ich kapital bilan 2013 yilda eston dasturchilari tomonidan tashkil etilgan bo'lib, u yangi ish boshlaganlar uchun ham, malakali treyderlar uchun ham juda qulay. Unda 330 ta valyuta juftliklari bilan savdo qilish mumkin va hozirgi kunda savdo oboroti salkam 500 million AQSH dollarini tashkil qiladi. Birjada akkaunt ochish uchun foydalanuvchi o'z electron pochtasini ko'rsatib, minimum olti simvoldan iborat bo'lgan parol o'ylab topishi kerak bo'ladi. Bu ma'lumotlarni kiritganingizdan so'ng, pochtangizga akkaunt aktivatsiya qilingani haqidagi ma'lumot keladi. Akkauntni verifikatsiya qilish uchun quyidagi ma'lumotlarni kiritish kerak bo'ladi:

ATUGOV R.H., KADULOV V.R.



- *Ismi-sharifi*
- *Qaysi mamlakatda yashaydi*
- *Tug'ilgan sanasi*
- *Manzili*
- *Bank rekvizitlari*
- *Shaxisni tasdiqlovchi hujjatlar skanlari*

Birjadagi hisob raqamidan pullarni chiqarish va pul qo'yish uchun quyidagi usullardan foydalanish mumkin:

- *Asosiy valyutalardan (Bitcoin, Ethereum, Dash, Litecoin va boshqalar)*
- *Dollarlardagi SWIFT-to'lovlardan*
- *Evrodagi SEPA-to'lovlardan*

Ammo evro bilan ishlash birja saytida keltirilgan ruyhatdagi mamlakatlar uchungina ruhsat etiladi.

Shaxsiy hisob raqamidagi pul vositalarini almashtirishni boshlash uchun “**Exchange**” bo'limiga o'tish kerak bo'ladi. **HitBTC** ko'pgina valyutalar bilan pul operatsiyalari amalga oshirishga imkon beradi. Ularning ichida eng aktuallari Bitcoin, Ethereum, Dash, Litecoin va boshqalardir. Savdo juftliklari ichida esa eng ko'p amalga oshiradiganlari BCH/BTC va BTC/USDT lardir. Bir sutkada amalga oshiriladigan pul operatsiyalari hajmi 150 million dollarga yetadi. Agar operatsiya darhol amalga oshirilsa, birja komissiyasi 0,1% bo'lib, boshqalari uchun 0,01% dir.

**HitBTC** birjasining afzalliklari:

- *Valyuta juftliklarining ko'pligi*
- *Pullarni fiat valyutalarda chiqarish mumkinligi*
- *Savdoni akkauntini verifikatsiya qilmasdan ham amalga oshirilishi mumkinligi*
- *Yuqori darajadagi hayfsizlik ta'minlanganligi*

**HitBTC** birjasining kamchiliklari:

- *Rus tilida ishlaydigan foydalanuvchilar uchun biroz noqulayliklar.*
- *Rusizabon mamlakatlar uchun evroda ishlash mumkin emasligi*

- *Boshqa birjalarga nisbatan savdo hajmi biroz kamchilligi*

**Kraken** birjasi o'z faoliyatini San Frantsiskoda 2011 yilda boshlagan va unda nafaqat kriptovalyutalar bilan, balki amerika va kanada dollarlari, britaniya funtlari hamda yapon iyenalari bilan ham savdo operatsiyalarini amalga oshirish mumkin. Ushbu birja **Bloomberg** terminalida kotirovka qilinadigan birinchi kriptovalyutalar birjasi bo'lgan edi. **Kraken** kriptovalyutalar birjasining bir kunlik oboroti dunyo miqyosida 5-7 chi o'rinda turadi. Ammo unda faqat eng taniqli kriptovalyutalar bilan 68 ta savdo juftligida savdo qilinadi va sutkali oborot 200 million AQSH dollriga yetadi. Komissiya miqdori esa savdo hajmiga bog'liq bo'lib, 1.6% dan 0.26% gacha yetadi. Birjada registratsiya qilinish uchun o'z e-mailingizni, login va parol kiritishingiz kifoya bo'ladi. Shundan so'ng kapchani kiritib, qoidalar bilan tanishib, ularga rozi bo'lish kerak bo'ladi. Keyin esa electron pochtaga kirib, qayd qilishni tasdiqlash qoladi holos. Birjada verifikatsiya qilinish uchun "**Get Verified**" vkladkasiga o'tish talab etiladi. Unda verifikatsiyaning beshta darajasi mavjud. Kredit vositalarga savdo qilish xuddi **Forex**ga o'xshash xolda amalga oshiriladi. *Birjaning afzalliklariga quyidagilarni kiritish mumkin:*

- ✓ Bu yerda marjinal savdo imkoniyati bo'lib, u orqali foydani anchagina miqdorga oshirish mumkin.
- ✓ Birja ko'p miqdordagi valyuta juftliklarini va ommabop kriptovalyutalarni taklif qiladi
- ✓ Kuchli himoya vositalari mavjud
- ✓ Planshet va mobil telefonlar orqali savdo qilish mumkin

*Birjaning kamchiliklariga esa quyidagilarni kiritish mumkin:*

- ✓ Ingliz tilini bilmaydigan foydalanuvchilar uchun bu birjada ishlash ancha murakkab kechadi
- ✓ Verifikatsiya jarayonini o'tmasdan turib savdoga kirishish mumkin emas
- ✓ Komissiya miqdori boshqa birjalarga qaraganda biroz kattaroq
- ✓ Depozitni rubl bilan to'ldirish mumkin emas
- ✓ Yandex-mani va Webmani bilan ishlab bo'lmaydi



Endi bitkoin va altkoinlar bilan ishlaydigan bir qancha valyuta almashtirish servislari bilan tanishib chiqishga va ularning afzalliklari hamda kamchiliklari bilan tanishishga harakat qilamiz. Bizlar uchun ishlash oson bo'lishini hisobga olib, rubl zonasida ishlaydigan mul'tivalyuta almashtirish punktlariga ko'proq ahamiyat beramiz. Albatta, katta halqaro servislari ham nazardan chetda qolmaydi.

**XCHANGE.CASH** halqaro valyutalar almashinuv servisida barcha actual kurslar va zahiralar saytda ko'rsatilib turiladi. Unda yordam va maslahatlar berish uchun on-line chat ham bor. Registratsiya esa oddiy va avtomatik ravishda amalga oshirilishi mumkin. Ish vaqti dam olish kunlarisiz yiliga 364 kun, almashinuvning minimal miqdori 5\$, ikki bosqichli referral to'lovlar amalga oshirilgan. Kriptovalyutalardan BTC, LTC, ETH, DASH, DOGE, ZEC bilan ish olib borilsa, fiat valyutalardan RUR, USD, Payeer, Perfectmoney, Bitcoin, Qiwi, Яндекс деньги, AdvCash, Exmo, Livecoin hamda Rossiya banklari bilan ishlash mumkin. Interfeysning tili inglizcha va ruscha bo'lishi ko'zda tutilgan. Forum esa **Bits.media** da bo'lib, *e-mail [xchange.cc@gmail.com](mailto:xchange.cc@gmail.com)*. Kompaniya bo'yicha ma'lumotlar: **XCHANGE.INC**, Pochta manzili: Suite 401-66 The Century Tower Bldg, 4th floor Ricardo J. Alfaro Ave, Panama City, Rep. of Panama, Telefon: +507 279-3266, Факс: +507 279-3250

**X-PAY.CC** xalqaro valyutalar on-line servisi bo'lib, sutka davomida va dam olish kunlarisiz ishlaydi. Unda chegirmalar, bonuslar va mukofotlar tizimi mavjud bo'lib, **BTC** kriptovalyutalari va fiat valyutalar bilan ishlash mumkin. Komissiyasi almashtiruv kursi tarkibiga qo'shiladi. Interfeysi ruscha va kontakt telefonlari [support@x-pay.cc](mailto:support@x-pay.cc).

**BANKCOMAT.COM** – valyutalar almashinuvi bo'yicha ishonchli servis bo'lib, barcha ommabop yo'nalishlar bo'yicha sifatli va teskor almashinuvni ta'minlab beradi. Barcha valyuta almashinuv operatsiyalari anonym ravishda amalga oshadi. Sutka davomidagi foydali, loyali va competent texnik xizmat ko'rsatuv amalga oshirilgan. PM, Okpay va ADVcash to'lov tizimlarining rasmiy hamkori bo'lib, BTC, LTC, ETH kriptovalyutalar va fiat valyutalar bilan ishlay oladi. Komissiyasi

almashinuv kursi tarkibiga qo'shilgan. Interfeys tili esa rus tilida. Kontaktlar E-mail: [support.client@bankcomat.com](mailto:support.client@bankcomat.com)

**24PAYBANK.COM** – electron va kriptovalyutalarning almashinuv servisi bo'lib, dam olish kunlarisiz va sutka davomida ishlaydi. Interfeysi ruscha bo'lib, saytning mobil versiyasi juda qulay tashkil qilingan. Hisob raqamlari va hamyonlar to'liq identifikatsiya qilingan. Valyuta almashinishining minimal kattaligi 3\$ bo'lib, BTC kriptovalyutasi va fiat valyutalar bilan ishlay oladi. Komissiyasi almashinuv kursiga qo'shilgan va kontakti: E-mail: [support@24paybank.com](mailto:support@24paybank.com)

**BAKSMAN** – to'lov tizimlari va kriptovalyutalar bo'yicha almashinuv servisi bo'lib, unda banklar va to'lov tizimlarining katta tanlovi mavjud. Almashinuvning minimal miqdori 250 rubl va doimiy mijozlar uchun bonuslar tizimi mavjud. Servis BTC va Ethereum kriptovalyutalri hamda fiat valyutalar bilan ishlay oladi. Interfeys ruscha bo'lib, kontaktlar: [baksman.supp@gmail.com](mailto:baksman.supp@gmail.com)

**KASSA.CC** – yagona valyuta almashinuv punkti bo'lib, almashinuvning minimal miqdori 0,01BTC, 3\$ va 150 rubldir. BTC kriptovalyutasi va fiat valyutalar bilan ishlay oladi. Interfeysi ruscha, inglizcha, nemischa, xitoycha va frantsuzchadir. Kontaktlari esa : E-mail: [support@kassa.cc](mailto:support@kassa.cc)

**INDACOIN** – Visa va Mastercard bank kartalati yordamida kriptovalyutalarni sotib olish va sotish mumkin. 24/7 rejimida tinimsiz ishlaydi. Bitkoinlarni Qiwi ga avtomatik ravishda sotib olish mumkin. Doimiy mijozlar uchun chegirmalar mavjud. Referal dastur bo'yicha har bir almashinuvdan 1% daromad olish ko'zda tutilgan. On-line chat orqali texnik yordam olish mumkin. Servis BTC va LTC kriptovalyutalari hamda fiat valyutalar bilan ishlash imkonini yaratadi. Interfeys ruscha, inglizcha, xitoycha va ispancha bo'lib, kontaktlar: [support@indacoin.com](mailto:support@indacoin.com)

**ALFACASHIER** – electron valyutalar va kriptovalyutalarni almashinuv servisi bo'lib, barcha operatsiyalar to'liq avtomatlashtirilgan. Referal dasturida 5% dan 20% gacha komissiya ko'zda tutilgan. BTC-e kodlari ham almashinuvga qabul qilinadi. BTC va LTC kriptovalyulalari bilan birgalikda fiat valyutalar ham qabul

qilinadi. Interfeys tili inglizcha, ruscha, nemischa va ispancha bo'lib, kontaktlar: [www.alfacashier.com/contact](http://www.alfacashier.com/contact)

**MATBEA** – Bitcoin bilan ishlash uchun juda qulay servis bo'lib, unda bitkoinlarni komissiyasiz sotib olish, uni bank hisoblariga va kartalarga chiqarish mumkin. Unda BTC dan tashqari, fiat valyutalar bilan ham ishlash mumkin. Interfeysi ruscha va inglizcha bo'lib, kontaktlari: [mail@matbea.com](mailto:mail@matbea.com)

**BITPAY** – bu servisning shtab-kvartirasi Djodjiya statining Atlanta shaxrida bo'lib, u kriptovalyuta xizmatlarining global o'yinchisi hisoblanadi. Servis valyuta almashinuvidan tashqari, to'lovlarni boshqara oladi va Bitkoinning yirik operatorlaridan biri hisoblanadi. U Microsoft, NewEgg, TigerDirect, Warner Bros. Records, PayPal, Global Payments va AlterNet Systems kompaniyalari bilan hamkorlik qiladi. Servisning New-York, San-Frantsisko, Sankt-Peterburg, Amsterdam va Argentinada ofislari mavjud. 22 nafar elektron tijorat firmalari bilan integratsiya qilingan. **BTC** kriptovalyutasi va fiat valyutalar bilan ishlay oladi. Interfeysi bir qancha tillarni o'z ichiga oladi.

**COINBASE** – halqaro kriptovalyuta operatorlaridan biri bo'lib, uning servislari orasiga birkoinning mul'tiplatformali hamyoni va kriptovalyutalar almashinuv servisi kiradi. Uning shtab-kvartirasi Kaliforniyadagi San-Framtsiskodadir. **Coinbase** ning foydalanuvchilari bitkoinni joriy bozor kursida, bank ko'chirmasi yordamida AQSH da va 18 ta Evrova davlatlarida sotishlari va sotib olishlari mumkin. **Coinbase** birkoinni saqlash, jo'natish va olish uchun elektron hamyonlar taklif qiladi. Valyuta almashinuv xizmatlaridan foydalanish uchun mijozlar bank rekvizitlarini ko'rsatishlari va ikki bosqichli autentifikatsiyadan o'tishlari kerak bo'ladi. Hozirgi paytda **Coinbase** da 2,1 million foydalanuvchi va 2,5 million hamyonlar bor. Servis BTC kriptovalyutasi va fiat valyutalar bilan ishlay oladi. Interfeysi esa mul'titilli bo'lib, kontaktlari: **Coinbase, Inc., a Delaware Corporation**

Endi qanday qilib kriptovalyutalarni havfsiz sotib olish texnologiyasini qadam-ba-qadam tahlil qilib chiqamiz va bu borada o'z fikrlarimizni bildiramiz. Xosirgi paytda pul kredit va moliya sohasida faoliyat yuritadigan insonlar bitkoin va

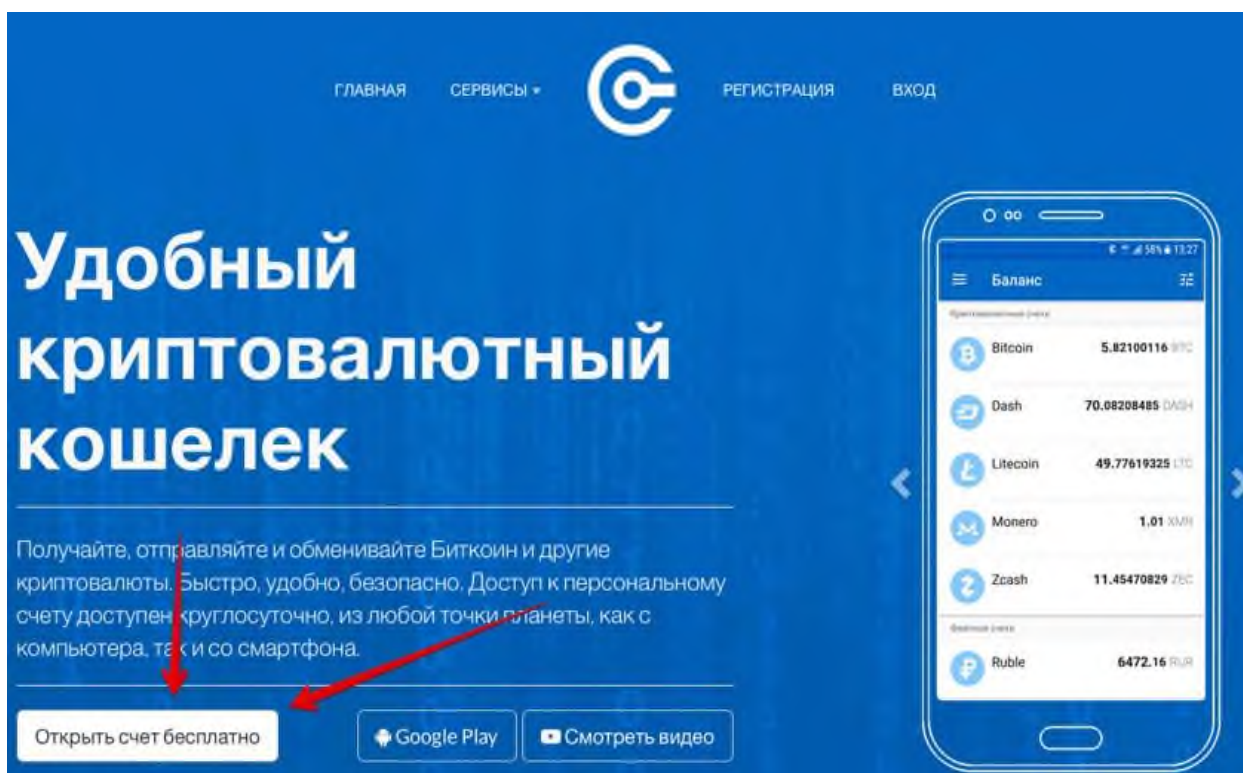
boshqa turdagi kriptovalyutalarni sotib olish jarayoni bilan qiziqadilar, ammo bu ish qanday amalga oshirilihi texnologiyasini juda yaxshi tushunmaydilar. Ularga yordam berish va ularni turli-tuman havf-hatar, yanglishish va moliyaviy yo'qotishlardan himoya qilish maqsadida ham ushbu bo'limni yoshishga bel bog'ladik. Ko'pchilik kriptovalyutalarni jahon miqyosidagi moliyaviy piramida, kapitalistik olamning tuzog'i, pul yuvishning zamonaviy usuli, uchchiga chiqqan moliyaviy firibgarlik deb hisoblashiga qaramasdan, dunyo miqyosida va respublikamizda ham uni sotib olmoqchi va shu orqali boyimoqchi bo'lganlar safi borgan sari kengaymoqda. Ammo shunga qaramasdan, kriptovalyutalar kursi o'garlik bilan o'sishda davom qilmoqda va unga yangidan-yangi investorlar, transmilliy korporatsiyalar va davlatlar ham tinimsiz ravishda tortilmoqda. Masalan, AQSH, Yaponiya, Xitoy, Venesuela, Belorusiya, Evropa hamjamiyati davlatlarida birjalar ishlab turibdi va bitkoinlarga oldi-sottilar yo'lga qo'yilgan. Rossiya va Qozog'stonda ham bu sohaga faol kirishish yo'llari va usullari aktiv muhokama etilmoqda. Chunki, 2010 yildan buyon bitkoin 50 tsentdan 20000 AQSH dollaridacha bo'lgan qiymatga o'sdi. Efirium esa 2015 yildan beri 1,2 dollardan 465 dollargacha kattalikka qimmatlashdi. Kimlardir buning oqibatida millioner va ba'zilar esa milliarder ham bo'lishdi. Bu sizga ham passiv (*kursning o'sishini kutib turasiz*) yoki aktiv (*kursda spekulyatsiya qilasiz*) investor bo'lib yaxshigina pul ishlab olish imkonini beradi. Kriptovalyutalarning bir salbiy tomoni ham bor – uni hech kim boshqarmaydi, shuning uchun uning kursi bir qancha sabablarga ko'ra tushub ketishi ham mumkin (*DDoS-hujum, katta oldi-sottilar, ba'zi davlatlarni undan tamoman voz kechishi, qonun bo'yicha taqiqlar va boshqalar*). Agar siz ham ommaviy kriptovalyutalar (*raqamli valyutalar*) olamiga kirishni va unda o'z omadingizni sinab ko'rmoqchi bo'lsangiz, quyida keltirilgan ko'rsatmalarga rioya qilishingiz maqsadga va aqlga muvofiq bo'lar edi. Demak, kriptovalyutalar olamida tezda boyib ketishingiz va xuddi shunday tarzda barcha pullaringizdan judo bo'lishingiz ham mumkin. Siz shunga tayyormisiz? Agar bu savolga “Ha” deb javob bersangiz, quyida keltirilgan maslahatlarni o'qing, aks

holda o'qimasangiz ham bo'ladi. Endi qanday qilib kriptovalyutalar olami bilan oshno bo'lish mumkinligini qadam-ba-qadam ko'rib chiqamiz:

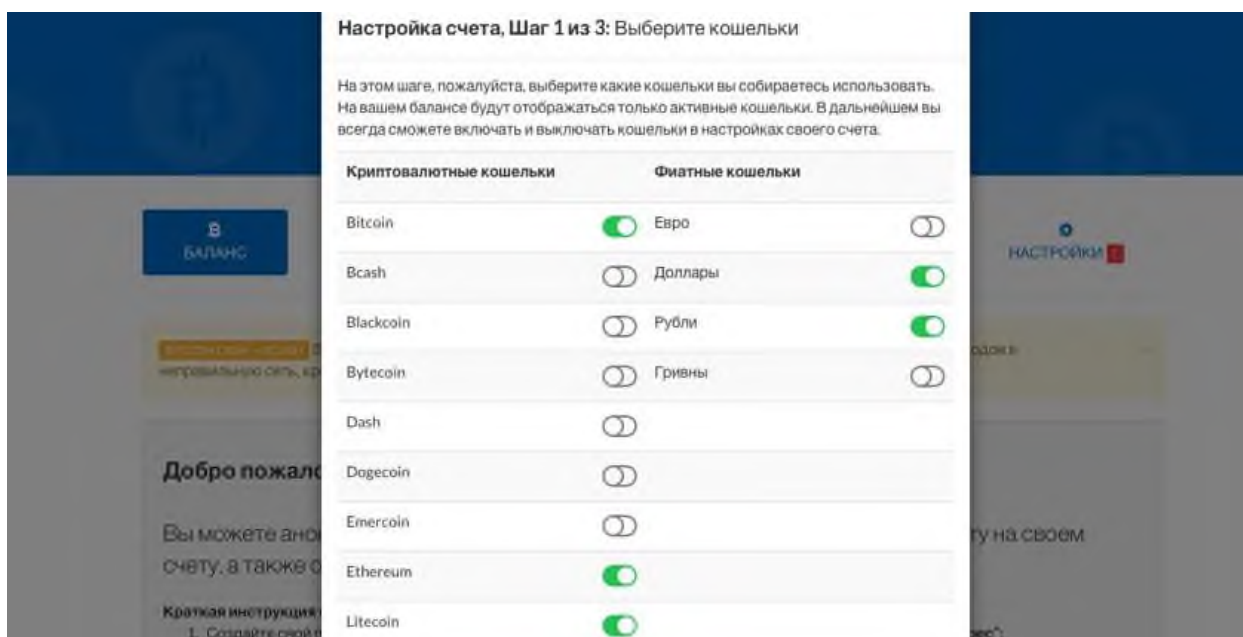
**Kriptohamyon ochish.** Bunda uch usuldan foydalanish mumkin:

- “*Dasturiy*” kriptohamyon ochish – masalan, **blokcheyn.info** va “**Криптонатор**” lardan foydalangan xolda.
- *Apparat hamyonlar* – **PIN** kodlar bilan himoyalangan bunday hamyonlar narxi 3-7 ming rubl turadi.
- *Qog'ozli hamyonlar* – bunda kalitlar mahsus saytlarda generatsiya qilinadilar va qog'ozga pechat qilib olinadilar.

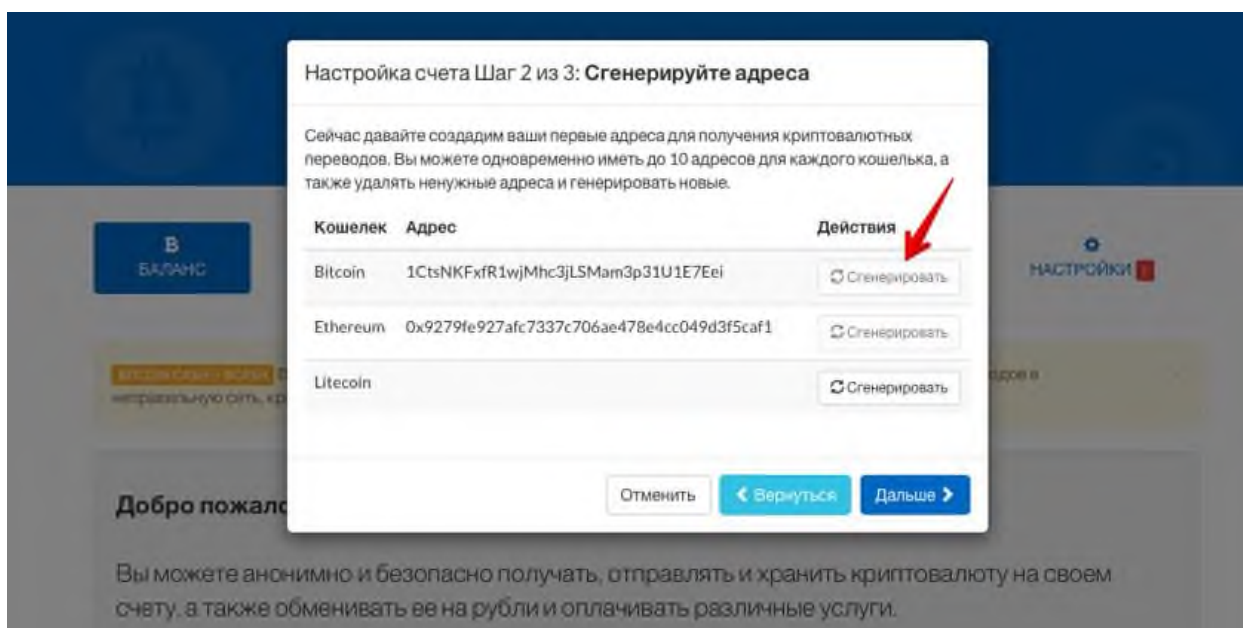
Komp'yuterimizda o'z hamyonimizni ochish uchun ko'pchilik foydalanuvchilar tomonidan tavsiya etilgan “**Криптонатор**” dan foydalanamiz va «**Открыть счет бесплатно**» tugmachasidan foydalanib, hisob-raqami ochamiz:



Shundan so'ng, pochta manzili va parolni kiritamiz, pochta manzilini tasdiqlaymiz va qanday kriptovalyutalarda to'lovni amalga oshirishimizni tanlaymiz (*ya'ni, bizni qiziqtirayotgan valyutani tanlaymiz*):



Endi «*дальше*» tugmachasini bosib, **Public Key** (*pul o'tkazmalari va operatsiyalar hisob raqami*) generatoriga duch kelamiz. Yuqorida biz uch turdagi kriptovalyutani tanlaganimiz tufayli, bizda ularning har biri uchun kriptovalyutaning o'z adresi bo'ladi. Ularni generatsiya qilishni boshlaymiz:



Shundan so'ng, yangi ochilgan hisob raqamimizning havfsizligini ta'minlash uchun uning ikki faktorli avtorizatsiyasini sozlaymiz. Endi o'zingizning barcha valyutalaringiz balanslarini tekshirishingiz (*bunga fiat balyutalar ham kiradi*) va kriptovalyutalarni boshqa insonlarga yoki magazinlarga o'tkazishingiz mumkin. Ushbu operatsiyalar uchun komissiya miqdori o'tkaziladigan summaning 0,04% ni tashkil qiladi holos:

AYUPOV R.H., KABULOV V.K.



Rossiya federatsiyasida kriptovalyuta orqali internet to'lovini, mobil aloqa to'lovini o'tkazish, "Тройка" transport kartasini va boshqalarni ham to'lash mumkin.

Ammo hozirda sizning hisob raqamingizda hech qanday pul yo'q. To'lovni amalga oshirish uchun hisob raqamingizni bitkoin va efirlar bilan to'ldirishingiz kerak bo'ladi. «Криптонатор» da fiat hisob raqamlarini Яндекс.Деньги, bank kartasi AYUPOV R.H., KABULOV V.K.

va **Payeer** to'lov tizimi yordamida ham to'ldirish mumkin. Ammo buning uchun komissiya miqdori fiat hisob raqami to'ldirilganidan so'ng 5,9% ni tashkil qiladi:

Пополнить счет

Мы предлагаем различные способы пополнения вашего счета. Выберите нужный вам способ чтобы узнать условия.

Откуда пополнить

Яндекс.Деньги ☒ Банковская карта ☐ PAYEER ☐

За одну операцию можно пополнить счет на сумму от 100 руб. до 50 000 руб. Комиссия за пополнение 5,9% вкл. комиссию Яндекса.

На какую сумму пополнить?

Сумма к оплате (вкл. все комиссии)

Обратите внимание: После первого пополнения через Яндекс.Деньги с нового кошелька будет установлена 24 часовая блокировка на вывод средств со счета. Дальнейшие пополнения будут происходить без блокировки. [Подробнее](#)

Продолжить Отменить

Endi hisob raqamimizdagi pullarni kriptovalyutaga aylantiramiz. Buning uchun sotadigan valyutamizni va sotib olmoqchi bo'lgan valyutamiz turini tanlaymiz va kerakli valyutani qancha pulga sotib olishimizni ko'rsatamiz:

В БАЛАНС ОТПРАВИТЬ ЗАПЛАТИТЬ **ОБМЕНЯТЬ** ИСТОРИЯ НАСТРОЙКИ

Продать

Выберите валюту

Сумма на продажу (0 RUR доступно)

Купить

Выберите валюту

Сумма к покупке

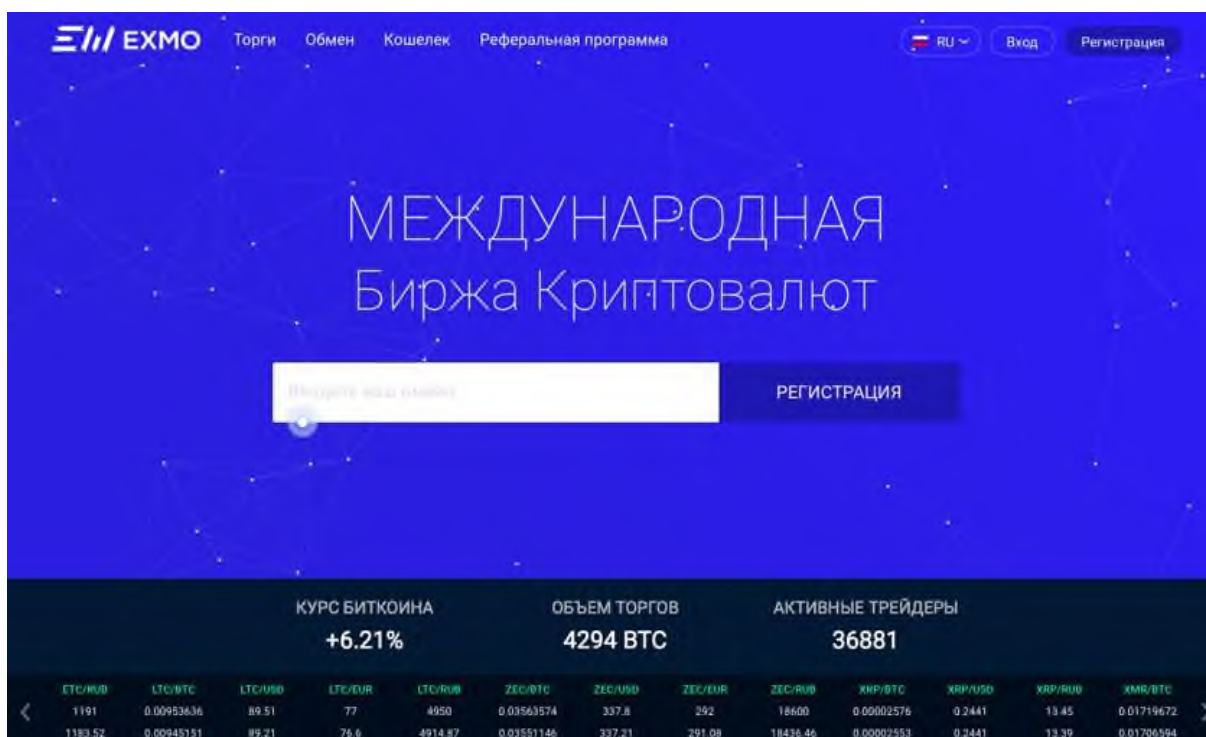
1 RUR = 0.00003855 ETH

Продолжить

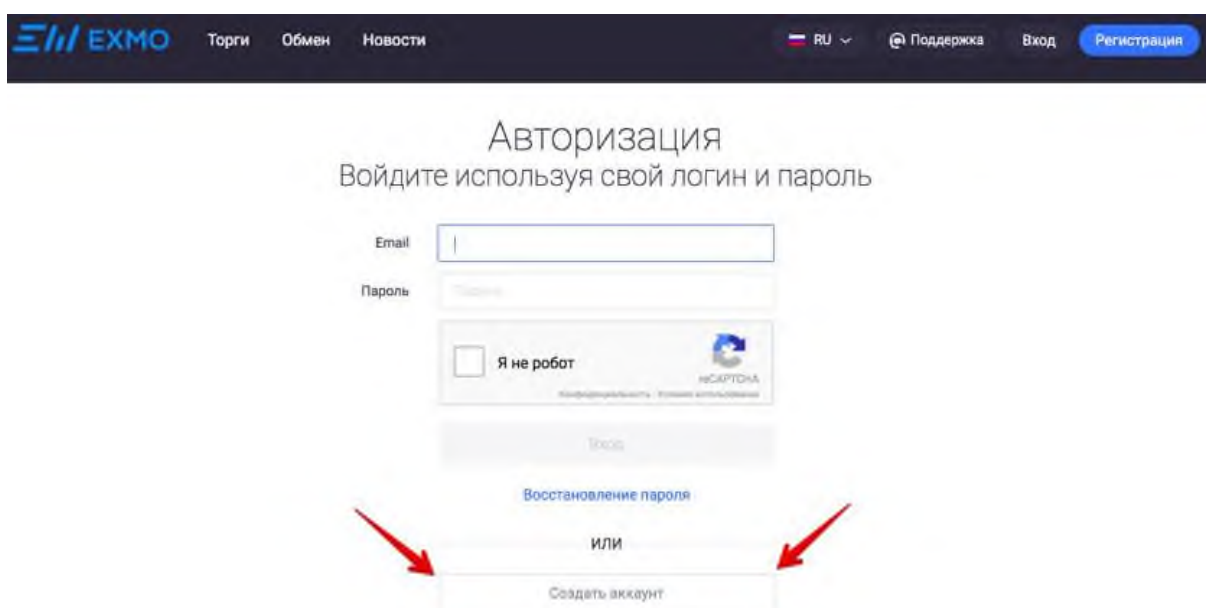
Birjadan valyuta sotib olish jarayoni biroz murakkabroq, chunki hozirgi davrda (2017 yilda) O'zbekiston va Rossiyada kriptovalyuta sotadigan birjalar mavjud emas. Shuning uchun havfsizlikni ta'minlashga puhta talablar qo'ygan Yapon birjalari **Bitflyer**, **Zaif**, **Coincheck** lardan kriptovalyuta sotib olish tavsiya qilinadi.



Evrova Ittifoqida faoliyat ko'rsatadigan bijjalarga misol sifatida Lyuksemburg birjasi **Bitstamp** yoki Britaniyaning **Exmo** birjasini ko'rsatish mumkin. **Exmo** birjasi bilan ishlashga harakat qilib ko'ramiz (*uning ruscha versiyasi ham mavjud*):



Endi bu birjada elektron hisob raqami (akkaunt) yaratib, login va parol o'ylab topish kerak bo'ladi. Ushbu yumushlarni tugallaganimizdan so'ng bizga birja hamyoni ochiladi. Pochta orqali akkauntingizni tasdiqlashni unutib qo'ymang.



Bu hamyonda siz turli valyutalar va kriptovalyutalardagi o'z balansingizni ko'rishingiz mumkin. Birja orqali esa bir valyuta turini boshqasiga almashtirishingiz yoki ularni sotishingiz, birja savdolarida ishtirok etishingiz

AYUPOV R.H., KABULOV V.K.

mumkin. Bunda xuddi oddiy birjalardagi kabi kurslar qandayligini kuzatishingiz, bitkoin sotib olish uchun ariza (*zayavka, order*) qoldirishingiz mumkin. Bunday arizalar darxol bajariladi.

The screenshot displays a trading interface for Bitcoin (BTC). At the top, there are tabs for 'По лимиту' (Limit) and 'По рынку' (Market). Below these, there are two main sections: 'Покупка, BTC' (Buy, BTC) and 'Продажа, BTC' (Sell, BTC). Each section contains input fields for 'Количество' (Quantity), 'Цена' (Price), 'Итого' (Total), 'Комиссия' (Commission), and 'Остаток' (Balance). Below the input fields are buttons 'Купить BTC' (Buy BTC) and 'Продать BTC' (Sell BTC). Red arrows point from these buttons to the 'История торгов' (Trade History) section at the bottom. The 'История торгов' section contains a table with columns: 'Дата/время' (Date/Time), 'Операция' (Operation), 'Цена' (Price), 'Количество' (Quantity), and 'Сумма' (Sum).

Дата/время	Операция	Цена	Количество	Сумма
27.11 08:10	buy	9480	0.00916562	86.6900776
27.11 08:10	buy	9480	0.00214979	20.3800092
27.11 08:10	buy	9480	0.001	9.48
27.11 08:10	sell	9476.8	0.88	8339.584

Savdo operatsiyalari bo'yicha komissiya 0,2% ni tashkil qiladi.

Agarda kurs biz uchun foyda keltiradigan darajada bo'lsa, bitkoinlarimizni birja orqali sotishimiz ham mumkin. Buning uchun qancha kriptovalyuta sotmoqchi bo'lganimizni, kurs bo'yicha narxini kiritib, bu operatsiyadan qancha foyda ko'rishimiz mumkinligini chamalab ko'ramiz (*komissiya narxini ayirib tashlagan xolda albatta*). Nihoyat order hosil qilamiz va uni tizimga kiritamiz. Uni shu zahoti boshqa treyderlar olib, savdoni boshlaydilar.

Покупка, BTC		Продажа, BTC	
Количество	0 BTC	Количество	1 BTC
Цена	0 USD	Цена	9480 USD
Итого	0 USD	Итого	9480 USD
Комиссия	0 BTC	Комиссия	18.96 USD
Остаток	0 USD	Остаток	-1 BTC
<a href="#">Купить BTC</a>		<a href="#">Продать BTC</a>	

Savdo natijasida ishlab topilgan mablag'ni **Payeer**, **advcash** larga o'xshash elektron to'lov tizimlari orqali chiqarib olish mumkin bo'ladi. Agarda siz pullarni bank kartasiga yoki **PayPal** ga chiqarmoqchi bo'lsangiz, u xolda identifikatsiya jarayonini amalga oshirishingiz kerak bo'ladi, ya'ni, o'zingiz haqingizdagi ma'lumotlarni tizimga kiritib, ularni passportingizning skanerlangan nushasi bilan tasdiqlashingiz talab etiladi:

Верификация	Проверка личности	Требования к документам
<p>1 Личность Не верифицирован</p> <p>2 Адрес Не верифицирован</p> <p>3 Соглашение Не верифицирован</p>	<p>Не верифицирован</p> <p>Имя: <input type="text"/></p> <p>Фамилия: <input type="text"/></p> <p>Отчество: <input type="text"/></p> <p>Дата рождения: <input type="text"/></p> <p>Серия и номер документа: <input type="text"/></p> <p>Действителен до: <input type="text"/></p> <p><a href="#">Цветной скан документа</a></p> <p><a href="#">Выберите файл для загрузки</a></p>	<p><b>Обязательные требования к документам</b></p> <ul style="list-style-type: none"> <li>Скан-копии или фотографии должны быть сделаны с оригинала, в хорошем качестве, все детали документов четко отображены.</li> <li>цветные скан копии или фотографии, выполненные на однотонном фоне.</li> <li>отображены целиком: обрезание краёв документа не допускается, все 4 (четыре) угла документа должны быть видны</li> <li>при этом не должны содержать посторонних предметов, объектов или надписей, которых нет на оригинале документа (например, скрепок, карандашей, пальцев и т.д.)</li> <li>отредактированные в графическом редакторе ИЛИ содержащие артефакты сканирования/фотографирования (след от вспышки, размытие) - не принимаются</li> <li>Файлы принимаются в форматах jpg или png, размером от 500kb до 5Mb</li> </ul>

Biror bir birjani tanlashdan avval albatta haridorlarning va soha bo'yicha forumdagilarning bu birja haqidagi fikrlari bilan tanishib chiqing. Kriptovalyutalar haqidagi dunyoviy yangiliklardan ham habardor bo'lish foyda berishi mumkin. Bu soha turli-tuman firibgarlardan ham xoli emas albatta. Ular turli birjalarning fishing sahifalarini hosil qilgan holda kriptovalyuta egalarining hamyonlaridagi pullarni o'g'irlashga harakat qiladilar.

Agar off-line rejimida ish olib borsangiz, bir qancha firibgarlarga duch kelish ehtimolidan xolis bo'lasiz. Ammo bunday punktlar hozircha unchalik ko'p emas. Bu punktlarga siz naqd pul bilan kelasiz va o'z hamyoningizga istalgan turdagi kriptovalyutani tushirib olasiz. Moskva shahrida off-line pul almashtirish punkti Yangi Arbatda mavjud. Agar raqamli valyutangizni sotmoqchi bo'lsangiz, uni **LocalBitcoins** ga tushirasiz (*bu tizim Rossiyada faqatgina VPN orqali ishlaydi*). Shundan so'ng, pul almashinuv tizimi uni ko'radi va sizning bitkoinlaringizni sotib oladi. Kriptovalyutalar sotish bo'yicha yana bir almashinuv punkti terminali Sankt-Peterburgdagi "**Ostrov**" biznes-markazida mavjud. Ushbu terminal orqali Bitkoin, Litekoin va Ethereum larni naqd pulga sotib olish mumkin.



Bu yerlarda zerikarli identifikatsiya jarayoni bo'lmagani tufayli kriptovalyutalar sotib olish uchun naqd qog'oz pullarni to'lash ham mumkin. Ammo komissiya miqdori juda ham katta – to'lagan pulingizning 4% idan 10% igacha. Shuning uchun ham on-line operatsiyalar xozircha nisbatan foydali deb hisoblash mumkin. 2017 yil yakunida Rossiya siyosatchilari (*Davlat dumasi*) kriptovalyutalar bilan ishlashga mo'ljallangan shahar qurish taklifi bilan chiqqanlar. Bundan asosiy maqsad – aholining va chet ellik turistlarni (*asosan Xitoyliklarni*) bu faoliyat turiga qiziqtirgan xolda yaxshigina mablag' ishlab olishdir.

Toshkentda ham 2018 yil 28 aprel kuni 25 mamlakat va 100 ga yaqin tashkilot vakillari ishtirokida blokcheyn va kriptovalyutalar bo'yicha Burunjahon sammiti o'tkazildi. Sammitning saytida (<http://tashkent.wbcsummit.org/>) "*MDH ning uchunchi o'rindagi eng yirik iqtisodiyoti – O'zbekistonga hush kelibsiz!*"

*Mamlakat iqtisodiy siyosatidagi o'zgarishlar va tayyorlanayotgan qonunchilik islohotlaridan kelib chiqib, O'zbekiston Markaziy Osiyoning yangi kriptopoytaxti sifatida tanlandi* ", deyilgan edi. Tashkilotchilarning fikricha, Toshkentda bo'lib o'tgan blokcheyn va kriptovalyutalar bo'yicha Burunjahon sammiti investitsiyalar va yangi loyihalarni amalga oshirish uchun bir yahshi imkoniyat bo'ldi. Ishtirokchilar *International Hotel Tashkent* mehmonxonasida raqamli iqtisodiyot, jumladan, ma'lumotlar mahfiyligi, blokcheyn-texnologiyalarni qo'llash, mayning, kriptovalyutalarni saqlash va almashtirish masalalari bo'yicha qizg'in muhokamalar o'tkazishdi. Sammitda Qozog'iston, Latviya, Gollandiya, Isroil, Bahrayn, Yangi Zelandiya, Avstraliya, Rossiya, Nigeriya va boshqa davlatlardan kelgan blokcheyn va kriptovalyuta bo'yicha mutaxassislar qiziqarli chiqishlar qilishdi. Ushbu sammit doirasida O'zbekiston bo'yicha loyihalar taqdim etadigan **Uzbekistan ICO Show** tadbiri ham bo'lib o'tdi. Shuni ham aytish kerakki, O'zbekiston 2018 yil boshida kriptovalyuta yig'ish eng arzon tushadigan mamlakatlar ruyhatida uchinchi o'rinni egallagan. **International Business Times** nashri ekspertlarining hisoblashlaricha, Oz'bekistonda bir bitkoin yig'ish 1790 dollarga tushar ekan. Bu borada faqatgina Trinidad va Tobago (*1190 dollar*) va Venesuelagina (*531 dollar*) O'zbekistondan yuqori o'rinda turadi. Janubiy Koreya esa bitkoin yig'ish befoyda mamalakat deb topilgan, chunki bu mamlakatda bitkoin yig'ish narxi 26170 dollardir.

## **11. Kriptovalyutalar bozorining rivojlanishi**

Bitkoin narxining navbatdagi ko'tarilishi ortidan Finlyandiya markaziy banki bitkoin tizimini revolyutsion va ajoyib deb tavsiflagan xolda ilmiy izlanishlar turkumini e'lon qildi. Ushbu ma'lumotda jahondagi minglab kriptomaynerlar tomonidan qo'llab-quvvatlanadigan bitkoinning juda stabil ekanligi ta'kidlanadi. Shu munosabat bilan 2017 yilni qo'rqmasdan bitkoin yili deb aytish mumkin, chunki yil boshida uning narxi 1000 dollar bo'lgan bo'lsa, yil davomida 20000 dollargacha o'sish kuzatildi, kelajakda esa uning narxi 100 000 dollargacha ko'tarilishi mumkin ekan. Bunday ma'lumotni **JPMorgan Chase** amerika



moliyaviy xoldingi bosh direktori ***Delivering Alpha*** deb nomlangan bank konferentsiyasida aytib o'tdi (12/09/2017 yil). Ammo uning fikricha, kelajakda kriptovalyutalar bozori bir ko'pik sifatida juda katta miqdorga yetganidan so'g yorilib ketadi, chunki unga bo'lgan talab ko'pchilik xollarda sun'iy talabdir – u an'anaviy pullar bozori bilan to'liq integratsiyalashmagan. Kriptovalyutalar bozorining rivojlanishini qisqacha ravishda quyidagicha tavsiflash mumkin:

- Bitkoin tushunchasi birinchi marotaba 2008 yilda Satoshi Nakomoto ismli inson nomidan kiritilgan.
- Bitkoinning asosida electron zanjir orqali ma'lumotlar uzatish texnologiyasi – blokcheyn yotadi.
- Blokcheynning turli elementlari har xil komp'yuterlarda saqlanadi va ularning xaqiqiyliги aniq matematik algoritmlar orqali nazoratchi organlar ishtirokisiz tasdiqlanib turadi .
- 2017 yil 1 avgustda bitkoin ishlab chiqaruvchilar uning tezroq ishlaydigan analogi **Bitcoin Cash** ni yaratdilar.
- Bitkoinning kriptovalyutalar bozoridagi eng asosiy raqobatchisi rossiya-kanada dasturchisi tomonidan 2013 yilda ishlab chiqilgan kriptovalyuta ***Etherium*** yoki **Efir** hisoblanadi.

Kiptovalyutalar bozorining rivojlanishini 2000 yillar boshida ro'y bergan “dotcom” lar bo'yicha katta qiziqish va uning nima bilan tugagani bilan ham solishtirishimiz mumkin. O'sha davrda domen ismlari **.com** bilan tugaydigan texnologik kompaniyalar aksiyalariga juda katta qiziqish kuzatilgani tufayli, birjalarda zamonaviy nomlar bilan atalgan, **.com** domen nomi bilan tugaydigan, ammo amalda mavjud bo'lmagan kompaniyalarning aksiyalari faol sotila boshlandi. Bu firibgarlik ma'lum bo'lib qolganidan so'ng, dotcom kompaniyalarning aksiyalari juda ham tushib ketdi va ko'pgina kompaniyalar buning oqibatida xonavayron bo'ldilar. **CoinMarketCap** saytining ma'lumotlariga ko'ra, xozirgi paytda internetda 900 ga yaqin raqamli kriptovalyutalar mavjud. Bu bozorda yangi ishtirokchilar deyarli har kuni paydo bo'layaptilar va ularning barchasi ham yaxshi o'ylab tuzilgan bizner-rejaga ega yoki ular firibgar emas deb

aniq aytib bo'lmaydi. Ularning bankrot bo'lishi butun kriptografiya bozorining tushkunlikka uchrashiga olib kelishi mumkin. Ya'ni, sun'iy kriptovalyutalarning inqirozi o'z ortidan bitkoin, laytkoin va efiriumlarning ham inqiroziga sabab bo'lishi mumkin. Lekin shuni ham aytish kerakki, kriptovalyutalar uchun yana katta bir havf davlat tomonidan ham kelishi mumkin va muqarrar. Moliyaviy analitik Djeyms Daymonning aytishicha, *“Valyuta bu davlat tomonidan birinchi navbatda yaratiladigan narsadir. Davlat esa valyuta aylanishini markaziy bank yordamida nazorat qiladi. Undan tashqari, davlat kim valyutaga egalik qilayapti, u qaerda turibdi va nimalarga sarf qilinishini bilishni istaydi”*. Xuddi shuning uchun ham Xitoy kriptovalyuta birjalarini yopayapti. Kriptovalyutalar qanchalik ko'p bo'lsa, davlat shunchalik faolroq uni nazorat qilishni xoxlaydi. Xozircha kriptovalyutalar yangilik bo'lgani uchun davlat undan foydalanishga chidab turibdi, ammo undan biror kimsa yoki tashkilot zarar ko'rgani aniqlansa yoki kimdir undan noqonuniy amallar uchun foydalansa, davlat shu zahoti uni yopib qo'yadi”. Masalan, 2015 yilda Rossiya moliya vazirligi *“pul surrogati”* chiqarganlar va uni sotishga uringanlarni yetti yilgacha qamoq jazosi bilan jazolashni taklif qildi. Pul surrogati termini kriptovalyutalarga ham tegishlidir.

**Quyida mamlakatlar miqyosida bitkoin tizimini elementlari (tarmoq ishtirokchilari) soni keltirilgan (2017 yil sentyabr xolati)**

1. AQSH	2567 (27,58%)
2. Germaniya	1688 (18,13%)
3. Frantsiya	657 (7,06%)
4. Xitoy	558 (5,99%)

5. Niderlandiya	445 (4,78%)
6. Kanada	378 (4,06%)
7. Noma'lum mamlakatlarda	332 (3,57%)
8. Angliya	322 (3,46%)
9. Rossiya	305 (3,28%)
10. Singapur	210 (2,26%)

Bitnodesning 14 sentyabr 2017 yilgi ma'lumotlari

2017 yil sentyabr oyida Rossiya moliya vaziri Anton Siluanov kriptovalyutalarni boshqarish bo'yicha qonun loyihasini shu yilning oxirigacha tayyorlashini bildirdi. Dekabr oyida Moskvada o'tkaziladigan slyotda bu masalaga birmuncha oydinlik kiritilishi mumkin. Ministrning aytishicha, bu xujjatni tayyorlashdan asosiy maqsad – mamlakatda aldanib qoladigan investorlar bo'lmasligiga erishishdir. Moliyaviy bozorlar bo'yicha davlat dumasi komiteti raisi Anatoliy Aksakov ham kriptovalyutalar bo'yicha qonun loyihasini yil oxirigacha qabul qilish mumkinligini bildirdi. Rossiya davlat banki kriptovalyutalarni raqamli mahsulot deb tan olgan xolda uni ham soliqqa tortish kerakligini bildirdi. Ammo kriptovalyutalar oltin zahiralari bilan ta'minlanmaganligi tufayli, ularni ko'plab miqyosda chiqarish valyuta bozoriga parokandalik olib kelishi mumkin. Insonlar pul o'rniga kriptovalyutalarni ommaviy ishlata boshlashsa, u asta-sekin pulnini o'rnini egallab olishi mumkin. Rossiyadagi va dunyoning bir qancha mamlakatlaridagi huquq-tartibot organlari ko'pchilik kriptovalyuta birjalariga internet orqali kirishni yopib qo'yayaptilar – ularning fikrlaricha raqamli



valyutalarning anonimlik xususiyati tufayli “*kriptovalyutalar narkotik moddalar, qurol-yaroq, qalbaki xujjatlar savdosida va boshqa turdagi noqonuniy jinoyat ishlarida qo'llanilishi mumkin*”. Ya'ni, nazorat qilib bo'lmaydigan trahschegaraviy kriptooperatsiyalar terrorizmni moliyalashtirish uchun xizmat qiladi. Ammo, kriptovalyutalar to'liq anonym emasligi g'arb davlatlaridagi politsiya xizmatlari va maxsus xizmatlar amaliyotidan allaqachon ma'lum bo'lgan, chuni ular bitkoin-hamyonlar egalarini mahsus dasturiy ta'minot yordamida bemalol aniqlay oladilar. Masalan, 2017 yil boshida Daniya politsiyasi internet orqali narkotik moddalar zakaz qilgan va unga bitkoinlar yordamida pul to'lagan shaxsni aniqladi. Uning qancha pulga narkotik moddalar zakaz qilganini aniqlagan xolda bu shaxsni sakkiz yilga qamoq jazosiga xukm qilindi (*Berlingske nashriyotidan*). Bu operatsiyani amalga oshirish uchun *Chainanalysis* deb nomlangan amerika kompaniyasining shu nomdagi analitik dasturidan foydalanildi. Ushbu dasturni Daniyalik Yan Moller ishlab chiqqanligi aniqlandi. Lekin bu huquq-tartibot organlari tomonidan bitkoin-hamyonning egasi aniqlangan (*deanonimizatsiya*) birinchi xodisa emas.

Shuni ham ta'kidlash kerakki, bitkoin yaratuvchining kimligi xaligacha ma'lum emas, bu esa bundan eng avval kim foyda olgan va uning (*yoki ularning*) maqsadlari nima bo'lganini aniqlashga imkon bermaydi. Xuddi shuning uchun ham **Chronopay** kompaniyasining R&D-bo'limi boshlig'i *Dmitriy Artimovich* quyidagi fikrni bildiradi: “*Bitkoin uni dollar yoki boshqa turdagi valyutaga almashtirish mumkin bo'lmagani qadar mavjud bo'ladi. Hech qanday mamlakat o'z moliyaviy tizimini qandaydir tushunarsiz valyuta ixtiyoriga berib qo'ymaydi. Chunki bitkoinning rivojlanishi bir qancha savollarni yuzaga keltiradi: Kim bu ishni moliyalashtirgan? Kim birinchi marta kriptovalyuta almashtirish punktlarini tashkil qilgan? Kriptovalyutalar ko'proq kimning qiziqish va intilishlariga mos keladi? Kriptovalyutalar kimlarning maqsadlarini amalga oshirish uchun xizmat qiladi? va xakazolar. Boshqa tomondan qaraganda, jahondagi ko'pchilik moliyaviy oqimlarni mahsus xizmatlar nazorat qilishga intiladilar. Shuning uchun ham kriptovalyutalar tizimi o'z-o'zidan paydo bo'lgan degan fikrga ishonish qiyin. Balki uni g'arb mahsus xizmatlari tashkil qilib, uni qandaydir usulda nazorat*

*qilish va boshqarish mexanizmini ham ishlab chiqqan bo'lsalar ajab emas". Lekin CyberFund blokcheyn platformasini ishlab chiqqan dasturchi Valeriy Litvin bu borada boshqacha fikrni bildiradi: "Binkoinni mahsus xizmatlar ishlab chiqqan va uni bekdooor (tizimni izdan chiqarish imkoniyati) bilan ta'minlaganlar degan fikr dunyo miqyosidagi fitna nazariyasi kabi asosga ega emas, chunki blokcheyn loyihalarning bacha kodlari ochiq va ularni istalgan inson (yoki tashkilot) istalgan paytda tekshirib audit qilishi mumkin. Undan tashqari, xuddi bitkoin singari boshqa turdagi kriptovalyutalar ham paydo bo'layapti va ular ham blokcheyn texnologiyasi asosida yaratilgan. Ular bitkoinga nibatan ancha katta bo'lgan anonimlilik darajasiga ega bo'lishlari mumkin". Ammo dunyodagi yirik va ko'zga ko'ringan moliyachilarning kriptovalyutalar bo'yicha turli-tuman munozaralariga qaramay, raqamli kriptovalyutalar borgan sari ko'proq jahon iqtisodiyotiga ta'sir qilayaptilar va ularga bo'lgan investitsiyalar miqdori kun sayin ortmoqda. Nima uchun kriptovalyutalar kursi juda tez o'zgaradi va unga egalik qilishda tavakkalchilik miqdori juda ham katta miqdorda degan savolga quyidagicha javob berish mumkin. Moliyaviy ekspertlarning fikricha, kriptovalyutalarning ortida real iqtisodiyot, tovar va xizmatlar harakati, kapital harakati, to'lov qobiliyati pariteti kabilar turmaydi, xuddi shu tufayli ham kriptovalyutalar ularni boshqarish bo'yicha yangiliklar va shu kabi boshqacha stress faktorlarga juda ham sezgirdirlar. Shu tufayli turli mamlakatlarda kriptovalyutalarga turlicha yondoshuv mavjud: Ba'zi mamlakatlarda ular umuman nazorat qilinmaydilar, boshqalarida esa kriptovalyutalar allaqachon to'lov vositasi sifatida ishlatiladilar. Bu yo'nalishda umumjahon qonunlari paydo bo'lishi ham ehtimoldan holi emas. Kriptovalyutalar bozorining kelajakdagi xolatiga nazar salsak, bu bozorda tavakkalchilik xali-hanuz ancha yuqori bo'ladi. Shuning uchun ham uzoq va qisqa muddatli perspektivalarda ko'tarilish va pasayishga tayyor bo'lgan investorlarga bu bozorda o'ynash tavsiya etiladi.*

Quyida nima sababli kriptovalyutalar kursi tez-tez va shiddatli tarzda o'zgarishining yana boshqa bir qancha sabablari keltiriladi: Bularning birinchisiga xuddi oddiy pullar va qimmatli qog'ozlar bozorida bo'lgani kabi "ruhiy"

faktorlarni kiritishimiz mumkin. Masalan, investorlarni kutish, talabning vaqtinchalik ko'payib ketishi, talab o'sishining sekinlashuvi, juda tez o'sishdan so'ng charchoqlik xolati kabilar. Kriptovalyutalar bozorining boshqa turdagi aktivlar bozoridan asosiy farqi uning iqtisodiyot bilan uzviy bog'liq emasligidir. Mamlakatlar iqtisodiy hayotiga bitkoinlar kursining o'sishi yoki kamayishi xozircha ta'sir qilmaydi. Aksincha, dollar kursi tebranishi yoki neft narxi o'zgarishi iqtisodiyotga katta ta'sir ko'rsatadi. Ikkinchi sabab, kriptovalyutalarning yangi raqamli valuta turiga mansubligidir. Ko'pchilik uning nimaligini juda yaxshi tushunmaganligi uchun informatsion o'yinlar vositasida kriptovalyutalar kursini ko'tarish yoki tushirib yuborish mumkin. Bunda ommaviy axborot vositalari va ijtimoiy tarmoqlar katta ahamiyatga ega. Internetdagi qandaydir yangilik uning kursini tushirsa, boshqasi kursni ko'tarib yuboradi. Bu boradagi ko'pchilik ma'lumotlarni tekshirishning o'zi ham katta muammodir. Uchichi sabab sifatida kriptovalyuta dastur kodining yangilanishini (*hardfork*) keltirish mumkin. Kurs ma'lum maksimal darajaga yetgandan so'ng oldi-sotti vaqtincha to'xtatilishi mumkin, ammo bu umumiy xolatga katta ta'sir ko'rsatadi. Bitkoinning kursi juda ham o'zgaruvchan (*volatil*) bo'lgani uchun yirik investorlarning savdoga aralashuvi kursni anchagina o'zgarishiga olib keladi. Bu esa bitkoin puffagi xali bir necha bor kattalashishi va kichiklashishi mumkinligini anglatadi. Bitkoin kursi qachon stabillashishini xozircha hech kim bashorat qila olmaydi, shuning uchun bitkoin egalariga sabr qilish tavsiy etiladi.

Qaysi kriptovalyutani sotib olish kerak va qaysisini sotish kerak degan savolga javob berish ham juda murakkab masala. Ammo hozirgi sharoitlarni hisobga olgan xolda bitkoindan voz kechish ham unchalik to'g'ri bo'lmas. Negaki xozirgi paytda investorlar unga juda qattiq ishonadilar. Bitkoinga bo'lgan ishonch ***bitcoin cash*** va ***bitkoin gold*** ga bo'lgan ishonchga nisbatan ancha katta miqdorda. Undan tashqari, bitkoinning boshqa koinlarga nisbatan ishonch zahirasi anchagina kattaligini payqash mumkin. Agarda eng ommabop raqamli valyuta – bitkoinga al'ternatuva qidirilsa, u xolda bir qancha variantlarni taklif etish mumkin. Masalan, bitkoin daromad darajasi bo'yicha bir qancha kriptotokenlardan quyiroqda yuradi.

Misol uchun, **Stratis (STRAT)** ning narxi 2016 yil iyulidan buyon **ICO** tashkil qilingandan keyin 600 barobarga o'sgan bo'lsa, xuddi o'sha davrda bitkoin bor-yo'g'i 30 barobarga o'sgan. **SpectroCoin** (*kriptovalyutalar birjasi*) narxi esa 2017 yil yanvaridan buyon 400 barobarga o'sgan. Expertlarning fikricha, 2018 yil ham kriptovalyutalar uchun oldingi yilga o'xshash buhonli bo'ladi. Rossiyadagi **Wirex** kriptobankining asoschilaridan biri Pavel Matveevning fikriga ko'ra esa, 2017 yil oxiridagi tendentsiyalar bitkoin narxi 8000 dollargacha tushishini anglatadi. Boshqa expertlar esa bitkoinning narxi 2018 yil davomida 50 ming dollargacha o'sishini bashorat qilishadi. 2018 yilda bitkoin (**BTC**) ning narxiga Yaponiya, Xitoy, Belorusiya, Venesuela, Rossiya va dunyoning boshqa yetakchi kriptoiqtisodiyotli davlatlarida tegishli qonunlarning qabul qilinishi katta ta'sir ko'rsatishi mumkin. **Sidechain** (*biror-bir kanalning yoki qurilmaning qandaydir ko'rsatgichlarini boshqa bir qurilma yoki signal vositasida boshqarish usuli*) texnologiyasining ommaviy ravishda tadbiq etilgan xolda institutsional investorlar xuddi entuziastlar kabi bitkoinga butkul ishonib qolishlari mumkin bo'ladi va natijada ular bitkoinning kursi oshishiga ishqiboz bo'lib qoladilar va xuddi shu yo'sinda o'ynaydilar. Bu xolda esa bitkoinning ehtimoliy narxi 100 ming dollargacha ko'tarilishi mumkin bo'ladi. Bitkoinning kelajagi to'g'risida al'ternativ pessimistic bashoratlari ham mavjud. Masalan, amerikalik iqtisodchi Djefri Sakks ning **Boston Globe** da yozishicha bitkoin o'ziga xos moliyaviy puffak bo'lib, uning kursi insonlar ishonchiga va tezda boyib ketishga bo'lgan ishtiyoqiga bog'liqdir. Uning fikriga ko'ra, davlat hech qachon pul emissiyasiga bo'lgan nazoratni qo'ldan chiqarishga rozi bo'lmaydi va kriptovalyutalar bozorini boshqarish bo'yicha faol tadbirlarni amalga oshira boshlaydi. **Morgan Stanley** banki analitigi Djeyms Fasett **Business Insider** nashriyotiga bergan intervyusida “... agar kriptovalyutadan to'lov vositasi sifatida foydalanishning imkoni bo'lmasa, uning hech kimga keragi bo'lmay qoladi va narxi ham keskin tushib ketadi. Davlat organlari ham xuddi shuni amalga oshirish istagidalar” degan fikr bildirgan. Ammo, bizning fikrimizcha, kriptovalyutalarning kelajagi qanday bo'lishidan qat'iy nazar, 2018 yilda kriptovalyuta ajiotaji davom etaveradi.

Xozirgi paytda kriptovalyutalar yordamida mablag' ishlab olishning bir qancha usullari bo'lib, ular ichida ommaviyroq'i – bitkoinlarni naqd pulga sotishdir. Rossiyada bir guruh insonlar ushbu operatsiya orqali 500 million rublni naqdlashtirganlar. 2017 yilda ba'zi bir Rossiylik fuqarolar bitkoin sotib olish uchun kvartiralarini ham sotganlar. Xatto lo'lilar ham bitkoinga o'xshash tangalarni naqd pulga sotayotganlari kuzatilgan. Dindorlarning fikrlaricha, kriptovalyuta iqtisodiyotda foyiz mexanizmining amal qilishi tufayli, pul massasining real material resurslardan ajralib qolishining yana bir turidir. Ammo yahudiylar o'zlarining kriptovalyutalarini chiqarishga ulgurdilar. 2017 yil iyun oyida **Bitcoen** deb nomlangan yahudiy kriptovalyutasi amalga kirdi. Yahudiylar jamoasining fikrisha, bu kriptovalyuta spekulativ operatsiyalar uchun emas, balki butun jahon yahudiylarining hisob-kitob operatsiyalarini amalga oshirish uchun yaratilgan. Ushbu yangi kriptovalyuta faqatgina yahudiy jamoasi tomonidan boshqariladi, ammo uni istalgan inson sotib olishi mumkin.

2017 yilda jahonda ilk bitkoin milliarderlari ham paydo bo'lishdi. Ular egizak aka-ukalar Tayler va Kameron Uinklvosslardir. Ular 2013 yilda har biri 120 dollardan bo'lgan bitkoinlardan 11 million dollarlik sotib olishdi va shundan so'ng kriptovalyutaning narxi 100 barobarga o'sdi. Natijada aka-ukalar bir yumalab milliarderga aylanishdi. Ammo ular o'z bitkoinlarini sotmasliklarini bildirdilar. Ular bitkoinni "*oltinning yaxshiroq ko'rinishi*" deb hisoblashlarini aytib, bitkoin narxi 2018 yilda 40 ming dollargacha ko'tarilishini bashorat qilishmoqda. 2018 yil boshida bitkoinning kapitalizatsiyasi 306,5 milliard dollarga yetdi. Bunday katta miqdordagi o'sishga bir qancha sabablar mavjud. Masalan, **CME** va **CBOE** chikago birjalarida kriptovalyuta bo'yicha f'yucherslar va optsionlar ishga tushirilmoqda, boshqa bir qancha mamlakatlarda esa kriptovalyutalar tan olinib, ular to'lov vositasi sifatida ishlatilmoqda, boshqa bir davlatlarda esa qonuniy baza ishlab chiqilmoqda. Yana bir sabab, dollarning raqamli analogini chiqarayotgan **tether Ltd** kompaniyasi yirik kriptovalyuta birjasi **bitfinex** bilan kelishgan xolda ta'minlanuvsiz raqamli dollar chiqarib, ulari bitkoinlarga investitsiya qilmoqda. Undan tashqari, yirik jahon bank sektorlari o'yinchilari, avtomobil ishlab

ATUFOV R.H., KADULOV V.R.

chiqaruvchilar va riteyl-gigant **Amazon** ham asta-sekin kriptobozorga kirib kelmoqda. 2017 yilning noyabrida Shveytsariyaning **Vontobel** banki ham bitkoinlar uchun mini-f'yucherslar chiqara boshladi. Yaponiyada esa bitkoin rasmiy to'lov instrumenti sifatida tan olindi. Xindistonda ham kriptovalyutalar boshqaruvi bo'yicha qonunlar ishlab chiqish jarayoni amalga oshmoqda. AQSH bitkoinni birja mahsuloti deb tan olgan va Evropa mamlakatlari ham kriptovalyutani boshqarish bo'yicha tartibotlarni amalga kiritdilar. Kanada va Lotin Amerikasida ham bu xolatlar kuzatilayapti. Bularning barchasi bitkoinning kursi o'sishini ta'minlab, uning jahon miqyosida tan olinayotganligini anglatadi. Bitkoinlarni ishlatish ruhsat etilmagan davlatlar junlasiga Bangladesh, Boliviya, Ekvador, V'etnam va Qirg'izistonni kiritish mumkin.

Ko'pchilik moliyaviy analitiklarning fikrlaricha va **Saxo Bank** bashoratiga ko'ra, 2018 yilda bitkoinning narxi 60 ming dollarga yetadi va uning bozor kapitalizatsiyasi 1 trillion dollardan ham oshib ketadi. Ammo **Saxo Bank** ning valyuta strategisi Djon Xardining fikricha bu vaqtga kelib, Rossiya va Xitoyning ruxsat berilmagan kriptovalyutalarga ta'qiq qo'yishi natijasida 2019 yillarda bitkoinning narxi ancha tushib ketishi mumkin. Natijada uning narxi 2019 yillarga kelib 1000 dollar atrofida stabillashadi. Xozirgi davrda nafaqat investorlar, balki boshqa soha mutaxassislari ham kriptovalyutalar bozoriga katta qiziqish bilan qaramoqdalar. Masalan, **TechCrunch** ning habar berishicha, xakerlar **NiceHash** kriptobirjasini buzib, undan 60 milliondan ko'proq dollar mablag'ni o'g'irlashga erishdilar. Natijada 5 mingdan ortiq bitkoin yo'qolishi kuzatildi. Belorussiya davlati "*Raqamli iqtisodiyotni rivojlantirish*" deb nomlangan dekret kuchga kirgandan so'ng, milliy darajada smart-kontraktkarni legallashtirgan dunyodagi birinchi mamlakat bo'ldi. Bu haqda belorussiya *Yuqori texnologiyalar parki* saytida habar berilgan. Ushbu texnopark tokenlar bo'yicha operatsiyalarni amalga oshirish bo'yicha loyihalarni hayotga tadbqiq qilish uchun mo'ljallangan tajriba maydoni hisoblanadi. Mamlakat prezidentining bildirishicha, dekret respublikada information texnologiyalari, kriptovalyutalarni va blokcheyn texnologiyasini rivojlantirishga hamda mamalakatga transmilliy **IT**-kompaniyalar kelishiga qulay

imkoniyatlar yaratadi. Uning aytishicha “Yangi dekret ICO larni, kriptovalyutalarni va smart-kontraktlarni (*blokcheyn texnologiyasi asosida kontraktlar tuzish va uni bardavom etishga mo’ljallangan komp’yuter dasturi*) qonuniylashtiradi”. Dekret tokenlar yaratish, ularni almashtirish, saqlash, joylashtirish, sotib olish hamda kriptobirjalar va kriptovalyutalar platformalari faoliyatiga doir hech qanday chegaralashlar va mahsus talablarni nazarda tutmaydi. Yuqori texnologiyalar parkining bildirishicha “*Jismoniy shaxslar tomonidan amalga oshiriladigan mayning faoliyati, tokenlarni sotish, almashtirish hamda joylashtirish tadbirkorlik faoliyati deb hisoblanmaydi va tokenlar deklaratsiya qilinmaydi. Mayning faoliyati, tokenlarni yaratish, sotish va sotib olish esa 2023 yilgacha soliqqa tortilmaydi*”. Ammo bu ish Belorussiyada elektr energiyaga bo’lgan ehtiyojni ancha oshiradi, chunki mayning juda ham katta elektr energiyasini talab qiladi. Shuning uchun ham mamlakatda nisbatan arzon elektr energiya ishlab chiqarishga imkon beradigan atom elektr stantsiyalari qurilmoqda va yana yangilarini qurish rejalashtirilmoqda (*Buni Rossiyaning “Atomstroyeksport” tashkiloti amalga oshirmoqda. Natijada 2019-2020 yillarga kelib atigi ikkita energoblok mamlakatga 2Gvt arzon atom elektr energiyasi ishlab chiqarib beradi*). Rossiya prezidenti ham 2018 yil 1 iyuligacha kriptovalyutalar aylanmasi va **ICO** haqidagi qonunlarni ishlab chiqishga topshiriq berdi. Chunki Rossiyada ham kriptovalyutalar bozorida ishlovchilar soni borgan sari oshib bormoqda. 2017 yilning dekabr oyi boshida Venesuela prezidenti Nikolas Maduro ham mamlakatda 100 mln **ElPetro** kriptovalyutasini chiqarish haqida topshiriq bergan. Ushbu kriptovalyuta mamlakatda chiqarilayotgan neft bilan ta’minlanadi – ya’ni **1 ElPetro** 1 barrel neft narxiga teng bo’ladi. Mamlakat rahbarining fikricha, **ElPetro** Venesuelaning “*pul suvereniteti*” ni ta’minlab berishi va pul oqimi hamda investitsiyalarni ko’paytirishi kerak. Boshqa barcha kriptovalyutalardan farqli o’laroq, bu kriptovalyuta Venesuelaning Ayakucho neft konidagi 5 milliard barrel neft bilan ta’minlanadi. Agarda kriptovalyuta loyihasi muvaffaqiyatsizlikka uchrasa, har bir kriptovalyuta egasi bir barrel (*yoki bir bochqa*) neft egasi bo’ladi. Hozirgi narxlarda bu 60 dollar degani. 2018 yil 20 fevralda sotuvga chiqarilgan bu

kriptoalyuta birinchi kunning o'zidayoq 735 mln dollarlik sotildi, bir hafta ichida esa bu miqdor 1 milliard dollarga yetdi. Muvaffaqiyatdan ruhlangan loyihachilar endi **PetroGold** kriptoalyutasini chiqarishni rejalashtirayptilar – bu kriptoalyuta esa oltin bilan ta'minlanadi. Agarda loyiha muvaffaqiyatli amalga ohsa, **Petro** ning kapitalizatsiyasi 6 milliard evroga yetishi mumkin. Frankfurt moliya va menejment maktabining professori Philipp Sandnerning fikricha, virtual bozordagi bu kriptoalyuta material boylik bilan ta'minlangan bo'lgani uchun bitkoinga nisbatan ancha stabil bo'lishi mumkin. Karakasdagi mas'ullarning fikrlaricha, ularning o'z mustaqil kriptoalyutalari halqaro valyuta bozorlari bilan yaqindan muloqot qilishga imkon beradi va chet ellardan moliyaviy mablag'larni jalb qila oladi. Har qanday xolatda ham **ElPetro** kriptoalyutasi chiqarishni virtual dunyidagi bir tajriba sifatida qabul qilsh mumkin. Agar bu yondoshuv o'zining samaradorligini ko'rsatsa, boshqa mamlakatlar ham iqtisodiyotni rivojlantirish uchun bu tajribadan foydalanishlari mumkin bo'ladi.

Evropada ham bunday jarayonlar davom etmoqda, masalan, Buyuk Britaniya o'z kriptoalyutasini chiqarishni rejalashtirayapti. Bu kriptoalyuta Britaniya funt-sterlingi bilan bog'liq bo'lib, markaziy bankning fikricha, u banklar o'rnini bosishi mumkin.





Bunday Angliya milliy kriptovalyutasi 2018 yilning oxirlarida chiqarilishini *The Telegraph* Markaziy bank mulozimiga ishora qilgan xolda ma'lum qilgan. Hozirda buni qanday qilib amalga oshirish muammolari ilmiy izlanish jarayonida o'rganilayapti. Ushbu kriptovalyuta bitkoinning analogi bo'lib, tranzaksiya texnologiyalaridan foydalanishni ko'zda tutadi. Markaziy bankning fikricha, bu kriptovalyuta britaniyaliklarga banklar xizmatidan voz kechib, o'z pullarini raqamli aktivlarda saqlash imkonini beradi. Kriptovalyuta yordamida katta tranzaksiyalarni amalga oshirish mumkin bo'ladi (*masalan, ko'chmas mulk sotib olish osonlashadi*). 2017 yil dekabr oyi oxirida Izroil davlati ham "**Elektron shakel**" deb nomlanadigan o'z kriptovalyutasini chiqarishini bildirdi. Bu bilan Izroil iqtisodchilari ikki muammoni hal qilishmoqchi: iqtisodiyotdagi naqd pul miqdorini kamaytirish va qora bozorga qarshi samaradorroq kurashish. Bu kriptovalyuta bitkoinning analogi bo'lmadi, balki Izroil milliy valyutasiga ekvivalent bo'ladi. Shuni ham aytish kerakki, hozirgi paytda jahondagi 500 ta eng yirik internet-magazinlardan atigi uchtasigina bitkoinni qabul qiladi. Agar jahon

valyuta bozoridagi bir kunlik valyuta operatsiyalari miqdori 5,4 trillion dollar bo'lsa, kriptovalyuta bo'yicha bir kunlik operatsiyalar hajmi bor-yo'g'i 3 milliard dollarga yetadi, xolos.



O'zbekistonda ham kriptovalyutani muomalaga kiritishdan avval uning qanday moliyaviy aktiv ko'rinishida qabul qilish va undan qanday tartibda foydalanish masalasini hal qilish lozim bo'ladi, ya'ni unga oddiy raqamli pul sifatida qarash kerakmi yoki uni yangi turdagi valyuta sifatida ko'rish kerakmi. Shundan so'nggina mamlakatda kriptovalyuta aylanishining xuquqiy asoslarini ishlab chiqarish mumkin bo'ladi.

## ***12. Kriptovalyutalar bilan qanday ishlanadi***

Kriptovalyutalar bilan ishlash amaliyotini kriptoolamda juda ma'lum va mashhur bo'lib ketgan bitcoin kriptovalyutasi misolida ko'rib chiqib, uni tavsif etamiz. Chunki qandaydir turdagi amaliyot bo'lmasa, bu ko'pchilikka unchalik tanish bo'magan olamda ishlashni tushunish ancha muncha murakkabroq bo'ladi. Bitcoin tarmog'iga ulangan har qanday foydalanuvchi unda o'zining 34 ta raqam

AYUPOV R.H., KABULOV V.K.

va simvoldan iborat bo'lgan bitkoin manzilini va unga mos bo'lgan 64 ta raqam va simvoldan iborat bo'lgan yopiq kalitini generatsiya qila oladi. Bunday bitkoin manzillardan biri quyida keltirilgan:

**12A3rdfgDfhgJkgRe4F6zHHTer45HHDfSFg**

Ushbu manzilga mos bo'gan yopiq kalit esa quyidagicha bo'ladi:

**Qwfdg354JJfshridg2F12A3rdfgDfhgJkgRe4F6zHHTer45HHDfSFg4KskS  
FgERT176Ge4Gs**

Huddi shu yopiq kalit egasigina yuqorida ko'rsatilgan manzildan birkoinlarni jo'nata oladi. Har bir bitkoin manzilga faqat bittagina yopiq kalit mos keladi va ular o'ta murakkab matematik formulalar orqali o'zaro bog'langan. Manzilni bilgan xolda unga mos bo'lgan yopiq kalitni topish nazariy jihatdan ham, amaliy jihatdan ham mumkin emas. Bitkoin tarmog'ining har qanday foydalanuvchisi mustaqil ravishda va tekinga istalgan sondagi bitkoin manzillar va yopiq kalitlarni yaratishi mumkin. Mumkin bo'lgan manzillarni juda ham ko'plab variantlari bo'lgani uchun ikki marta bir hil manzilni generatsiya qilish ehtimolligi deyarli nolga tengdir.

Misol uchun, Ravshan ismli tarmoq ishtirokchisi o'z yopiq kaliti yordamida bu yopiq kalitini hech kimsaga bildirmasdan turib, o'zining bitkoin manzilidan istalgan bitkoin manzilga pullar jo'natishi mumkin. Buning uchun u o'z kom'yuterida kerakli tranzaktsiyani hosil qiladi va uni yopiq kalit bilan imzolaydi. Bu tranzaktsiyani tarmoqqa jo'natishdan avval Ravshanning komp'yuteridagi bitkoin-dastur ushbu ma'lumotni bir qancha matematik formulalar yordamida qayta ishlaydi va natijada raqamli imzo deb ataladigan mahsus kodni generatsiya qiladi. Bu jarayon Ravshanning komp'yuteri tarmoqqa ulanmagan bo'lsa ham avtomatik tarzda bajarilaveradi. Raqamli imzo tranzaktsiya va yopiq kalitlarning konkret juftligi uchun unikal bo'ladi va u bank chekidagi imzoga o'xshab ketadi. Shundan so'ng Ravshan raqamli imzoni tranzaktsiya bilan birgalikda bitkoin tarmoqqa jo'natadi. Ravshanning raqamli imzosini olgan komp'yuterlar unga mos bo'lgan yopiq kalitni topa olmaydilar, chunki raqamli imzo yaratilayotganda juda ham murakkab matematik

formulalar yordamida hisob kitoblar bajarilgan. Ammo Ravshanning raqamli imzosi va uning bitkoin manzilidan foydalangan xolda raqamli imzo Ravshanning adresiga mos bo'lgan yopiq kalit yordamida yaratilganiga ishonch hosil qilish mumkin. Shunday qilib, tranzaktsiyaning ikkala tomonida ham kriptografik operatsiyalar bajariladi: bir tomonda raqamli imzo hosil qilinsa, ikkinchi tomonda raqamli imzo tekshiriladi. Bitkoin-tarmoqning barcha tugunlari barcha tranzaktsiyalarni tekshirishlari lozim, chunki bu ishni bajarish uchun hech qanday boshqa markaziy organning o'zi mavjud emas. Ravshanning haqiqiy yopiq birkoin manzili borligiga ishonch hosil qilinganidan so'ng, komp'yuter tizimi ushbu manzilda jo'natilish uchun mo'ljallanilgan pullar bormi yoki yo'qligini tekshiradi. Buning uchun tugunlar Ravshan ko'rsatgan manzildagi oldingi barcha bitkoin-tranzaktsiyalarning yozuvlarini skanirovka qiladilar. Bitkoin tarmoqning yaratuvchisi Satoshi Nakamoto ham agar tugunlar tranzaktsiyalarni ular olingan zahoti yozib qo'salar, jiddiy muammolar paydo bo'lishini yaxshi tushungan. Chunki har bir tranzaktsiya haqidagi ma'lumot bir tugunlarga oldinroq va boshqalariga keyinroq kelgandan so'ng, har bir manzilda saqlanayotgan bitkoinlar soni bo'yicha tushunmovchiliklar paydo bo'lishi mumkin. Tarmoq sinxronizatsiyasi muammosini hal qilish uchun Satoshi tarmoqning har bir tuguni ishtirok etishi mumkin bo'lgan mug'ombirona konkurs o'tkazilishi tashkil etishini taklif qildi. Konkursda ishtirok etayotgan tugunlar eng so'nggi tranzaktsiyalarni bloklar deb ataladigan ruyhatlarga yig'adilar. Blok hosil qilinganidan so'ng, unga mahsus kriptografik xesh-funktsiya **SHA 256** ni qo'llaydilar. Bu xesh-funktsiya istalgan qiymatga ega bo'la oladi va ularning asosida unikal 64-razryadli qiymatni generatsiya qiladi. Konkurs ishtirokchilari esa boshida bir qancha nollar bo'lgan xesh-funktsiyali blok tuzishga harakat qiladilar. Masalan, agarda konkurs shartlari bo'yicha boshida beshta nolli xesh-funktsiya topish talab qilinsa, u xolda quyida keltirilgan ikkita xesh konkursda g'alaba keltira olar edi:

**00000dg4JJfshridg2F12A3rdfgDfhgJkgRe4F6zrHHTer45HHDfSFg4KskS  
FgERT176Ge4Gs**

va

**00000RT4Ge4GsQwfdg354JJfshridg2F12A3rdfgDfhgJkgRe4F6zrHHTer4  
5HHDfSFg4KskS**

Xesh-funktsia qo'llanilganidan so'ng, qaysi blok kerakli bo'lgan nollarli natija berishini oldindan bilish nazariy jihatdan ham, amaliy jihatdan ham mumkin emas. **SHA 256** va boshqa shunga o'xshash xesh-funktsiyalar bir xil kirish qiymatlari uchun doimo bir xildagi natijalar beradilar. Shuning uchun konkursning har bir ishtirokchisi blok oxiriga tasodiviy sonni qo'shib qo'yadilar. Kriptografik xesh-funktsiyalar shunday tuzilganlarki, kirish ma'lumotlarining istalgan (*istalgan miqdordagi kichkina*) o'zgarishi barcha chiqish ma'lumotlarining – natijaning tasodifiy ravishda o'zgarib ketishiga olib keladi. Agarda tugunning birinchi harakati xeshda kerakli nollar bo'lgan muvaffaqiyatga olib kelmasa, u xolda tugun blok oxiriga qo'shilgan tasodifiy sonni boshqasiga o'zgartiradi va blokni yana bir marta xeshlashtiradi. Bunday urinishlar biror bir tugun xeshlashtirilganda kerakli sondagi nollar bo'lgan blok topilmaguncha qadar qaytarilaveradi. Bunday blokni topish tasodifiyotga bog'liq albatta, ammo bloklarni boshqalarga nisbatan tezroq xeshlashtira oladigan tugungina konkursda yutib chiqish uchun ko'proq imkoniyatga ega bo'ladi (*ya'ni kimning komp'yuteri zamonaviyroq bo'lsa va tezroq ishlasa, o'sha konkursda yutib chiqadi*). Bu xuddi lotoreya o'yiniga o'xshadi – kim ko'proq lotoreya sotib olsa, uning lotoreya o'yinida yutib chiqish ehtimolligi shuncha yuqori bo'ladi. Xesh boshida bo'lgan va konkursda yutib chiqish imkonini beradigan nollar soni bloklar orasidagi intervalga mos ravishda o'zgarib turadi. Agarda bu interval qisqarib ketsa, u xolda bitkoinning dasturiy ta'minoti konkurs shartlarini avtomatik ravishda o'zgartiradi. Ya'ni, kerakli natijani olish qiyinlashtiriladi – bloklarda ko'proq nollar bolishi talab etiladi. Agar bloklar orasidagi interval 10 minutdan katta bo'lib ketsa, u xolda masalaning murakkablik darajasi kamaytiriladi.

Kerakli natijani olgan va konkursda g'olib chiqqan tugun masala hal qilinganini va masala yechilganini bildirish uchun olingan blokni boshqa

tugunlarga jo'natadi. Shundan so'ng, tugunlar g'alaba qilgan blokni undagi tranzaktsiyalar bilan birgalikda o'zlaridagi blokcheyn nushasiga qo'shib qo'yadilar. Bu blok oldingi blok qo'shilgan vaqtdan boshlab bajarilgan barcha tranzaktsiyalarning rasmiy yozuvi bo'lib qoladi. Agar g'alaba qilgan blokda konkursning oldingi raundida tarmoqqa jo'natilgan ba'zi bir tranzaktsiyalar yo'q bo'lsa, u xolda ular keyingi raundga o'tadilar. Tranzaktsiyalar va tasodifiy sonlar bilan birgalikda blokcheynga qo'shiladigan har bir blok oldingi blokka ilovaga va bitkoin-tarmoqning holatini ko'rsatadigan ilovaga ham ega bo'ladi. Tarmoq xolatini hal qilish bo'yicha kelishuvga erishishning bu usuli, yechimini topish uchun juda ko'p olimlar bosh qotirgan "*vizantiya generallari masalasi*" ni hal qilib beradi. Mohiyatan aytganda, bu amal tarmoqning bir qancha ishtirokchilariga ishonish mumkin bo'magan xolatda tarmoqning ishonchliligini ta'minlash masalasini yechishdir. Tarmoqning bir qancha ishtirokchilaridan qabul qilingan bloklardan blokcheyn xosil qilish va kelishmovchiliklarni ko'pchilik printsipi asosida hal qilish bu muammoni yechib beradi.

Endi yuqorida tavsif etilgan konkursda ishtirok etishdan maqsad nima? degan savolga javob berishga harakat qilamiz. Gap shundaki, konkurs shartlariga mos bo'lgan kerakli blokni topgan tugun egasi (*konkret inson yoki insonlar guruhi*) qandaydir miqdordagi mukofotga ega bo'ladilar. Bu mukofot bitkoinning birinchi to'rt yilida 50 ta bitkoin tangaga teng bo'lgan edi. Ushbu mukofotni olish uchun konkursning har bir ishtirokchisi qayta ishlanayotgan tranzaktsiyalar ruyhatiga qo'shimcha tranzaktsiyani qo'shib qo'yishi kerak bo'ladi. Bu bilan u o'z manziliga yangi bitkoinlarni qo'shib qo'yadi. Konkret blok konkursda g'alaba qilganida va u blokcheynga qo'shilganida, yangi bitkoin tangalari blokda ko'rsatilgan manzilga jo'natiladi. Agarda tugun o'ziga joriy vaqtdagi mukofotlanuvdan ko'ra ko'proq bo'lgan bitkoin tangalarini qo'shishga harakat qilsa, u xolda blok boshqa tugunlar tomonidan tan olinmaydi. Bu ish (*yolg'onni rad qilish*) agarda tugunning xeshi kerakli sondagi nollarga ega bo'lgan taqdirda ham amalda bo'laveradi.

### ***Hulosa va takliflar***

Barcha ijobiy va salbiy fikrlarga qaramasdan, kriptovalyutalar va blokcheynlar texnologiyasi mavjud va u baholi-qudrat ishlab turibdi. Boshqacha soʻzlar bilan aytganda, kriptovalyuta jini Aloviddining sehrli chiroqchasidan allaqachon chiqib ketgan va uzoq vaqt davomida bu jin hali ham koʻza ichida deb oʻzimizni ovuntirishimiz maqsadga ham, aqlga ham muvofiq emas. Biznes esa kriptovalyutalarni ish jarayoniga tadbiq qilish uchun tayyor boʻlib boʻlgan, dunyo miqyosidagi katta-katta halqaro banklar esa kriptovalyutalarni va blokcheyn texnologiyalarni qanday qilib ishlatishni faol oʻrganmoqdalar. Moliyaviy texnologiya (*Fintex*) industriyasi blokcheynni zamonaviy iqtisodiyotning eng perspektiv trendlaridan biri deb hisoblashgacha bordi. Faqat bu texnologiyalarning huquqiy jihatdan aniqlamaganligi ularga keng miqyosda rivojlanishga imkon bermayapti. Oʻz navbatida, blokcheyn hamjamiyati barcha istovchilarga bu yangi tizimlarni oʻrganishga yordam berishga tayyordir (*adabiyotlar ruyhatidagi saytlar ruyhatiga qarang*). Biz ham sizni bu jarayonlarning passiv kuzatuvchisi emas, balki aktiv ishtirokchisi boʻlishga chaqirib, dunyoni yaxshi tomonga oʻzgartirish tarafdorimiz.

Oxirgi hulosa sifatida shuni aytishimiz lozimki, oʻzbek milliy valyutasi – soʻmni ham qisman yoki qandaydir chegaralangan optimal nisbatlarda kriptovalyutali koʻrinishga va uni bu bilan bogʻliq boʻlgan blokcheynga oʻtkazish mamlakatimizdagi bir qancha moliyaviy muammolarni muvaffaqiyatli ravishda hal qilish imkonini berar edi. Shu jumladan:

- ✓ Joriy bank operatsiyalarining shaffofligini va tezkorligini oshirish;
- ✓ Davlat sektori samaradorligini va uning ishlash tezligini oshirish;
- ✓ Ikkilamchi va yashirin bank sektorini yoʻq qilish yoki uni nazorat ostiga olish;
- ✓ Davlat apparatidagi byurokrtiyani yengish va korrupsiyaga qarshi samarador kurashish;



- ✓ Soliqlar to'lash jarayonini mukammallashtirish orqali, soliq to'lamaslik xolatlariga qarshi samarador kurashish;
- ✓ Kichik biznes va tadbirkorlikning rivojlanishiga yangi innovatsion imkoniyatlar yaratish;
- ✓ Kriptovalyutalar va **ICO** mexanizmlari yordamida halqaro valyuta-kredit resurslarini O'zbekiston iqtisodiyotiga keng miqyosda jalb qilish;
- ✓ Iqtisodiyotga bo'lgan dollar va boshqa valyutalar bosimini kamaytirish va shu asosda so'mning raqobatbardoshligini oshirish;
- ✓ **ICO** vositasida korxona, tashkilot, xususiy tadbirkorlar hamda jismoniy shaxslar uchun yangi, qulay va samarador kredit mexanizmlarini ishga tushirib yuborish;
- ✓ Moliya-kredit muassasalarining ishini yanada takomillashtirish;
- ✓ Kriptovalyuta, **ICO** va blokcheyn infratuzilmalarini yaratish orqali yangi ish o'rinlarini hosil qilish va zamonaviy information texnologiyalarni respublikamizga jalb qilish;
- ✓ Innovatsion jarayonlarni jadallashtirish;
- ✓ Ichki moliyaviy resurslarni ishlatishda mobillilikni ta'minlash va boshqalar.

Yana bir imkoniyat sifatida **World Wi-Fi** platformasi yordamida aholi uchun internetdan tekin foydalanish imkoniyatini yaratishni ko'rsatishimiz ham mumkin. Bu platforma "**Efir**" (*Ethereum*) kriptovalyutasi blokcheyniga asoslangan. **World Wi-Fi** platformasida uch tomon bo'ladi: internet foydalanuvchisi, router egasi va reklama beruvchi. Ularning har qaysisi ham tizimdan o'z foydasi ulushini oladi. Uyida router bor bo'lgan va internetga ulangan oddiy insonlarni tekin **Wi-Fi** o'ziga jalb qila oladi, chunki ular internetga qo'shimcha ulanish nuqtasini hosil qilib, unga boshqalarni jalb qiladilar va shu orqali pul ishlay oladilar. Ularga ish haqqi **WeToken** kriptotokenlarida keladi va ular bu tokenlarni real pullarga yoki kriptovalyutalarga almashtirib oladilar.

Kriptovalyutalar olamidagi yuqorida tavsif etilgan strategik va taktik xatti-harakatlarning muvaffaqiyatli ravishda amalga oshishi va rivojlanishi uchun,

bizning fikri ojizimizcha, hozirgi kunda mamlakatimizda to'rt xildagi asosiy yo'nalishlar taklif etish mumkin:

- Birinchi stsenariyda **bit so'm** kriptovalyutasi muomalaga chiqarilishi mumkin. O'zbek milliy valyutasini blokcheynga va raqamli formatga o'tkazish unga bir qancha afzalliklar berishi mumkin, ammo bu holda bir qancha muammolarni qonunchilik asosida to'g'ri hal qilish kerak bo'ladi. Masalan, ushbu blokcheynni kim boshqaradi va unga davlat maqomi beriladimi yoki u korporativ maqomga ega bo'ladimi. Bit so'm ichki va tashqi bozorda qanday ishlatiladi va kim tomonidan nazorat qilinadi - degan savollarga ham bank-moliya-kredit sohalari mutaxassislarini jalb qilgan holda konkret, ishonchga sazovor hamda aniq javob topish lozim bo'ladi.
- Ikkinchi yo'nalishda O'zbekistonning suveren davlat blokcheyn tizimi tashkil qilinadi va u o'zida turli moliyaviy institutlarning funktsiyalarini qamrab oladi. Bunday institutlar jumlasiga banklar, depozitariylar, pensiya fondlari, soliq idoralari va boshqalarni kiritish mumkin. Bu amal soliq to'lash va mablag'larni fondlarga o'tkazish ishlarini nisbatan osonlashtirish va to'liq avtomatlashtirish imkonini beradi.
- Uchinchi imkoniyat esa kriptovalyutani alohida tashkilotlarda yoki hududlarda hayotga tadbiq qilinadi va bu sohada yetarlricha amaliy tajriba to'planganidan so'ng, bu ish respublika miqyosida amalga oshiriladi (*masalan, O'zbekiston Respublikasidagi ochiq iqtisodiy xududlarda yoki chet ellik mutaxassislar ishlaydigan innovatsion qo'shma korxonalarda*).
- Oxirgi, to'rtinchi imkoniyat esa Rossiya Federatsiyasidagidek Markaziy bank tomonidan raqamli kriptovalyutalar bilan ishlashni amalga oshiradigan pilot loyihani ishga tushirishdir (*mastercheyn loyihasi*). Ushbu platforma bozor ishtirokchlarining elektron usulda o'zaro ma'lumot almashinishi va blokchenlarda identifikatsiya qilinishi uchun mo'ljallangandir. Bu tizim asta sekin, kriptovalyutalar bilan ishlash tajribasi oshib borgan sari bir qancha davlat interaktiv xizmatlarining ham navbatma-navbat blokcheynga o'tkazilishini ta'minlashi mumkin.

Respublikamizda kriptovalyuta bo'yicha malakali mutaxassislarning juda kamligi va bu sohadagi tajriba ozligini hisobga olgan tarzda bu yo'nalishda malakali mutaxassislar tayyorlashni ham amalga oshirish zamona talabi bo'lib qolmoqda (*bu taklif oily va o'rta mahsus ta'lim vazirligiga, iqtisodiyot universitetiga, moliya institutiga hamda bank-moliya akademiyasiga tegishlidir*). Lekin blokcheyn texnologiyalarni hayotga tadbqiq qilish va o'zbek kriptovalyutasini chiqarich innovatsion g'oyasini qadam ba qadam amalga oshirish hozirdanoq boshlab yo'lga qo'yilishi kerak bo'lgan hayot taqozosidir. Chunki dunyodagi ko'pchilik rivojlangan mamlakatlar o'zlarining milliy yoki korporativ kriptovalyuta loyihalarini amalga oshirmoqdalar va ular keyinchalik barcha raqamli kriptopullarga egalik qilib, boshqa mamlakatlarni bu jarayondan siqib chiqarishga harakat qiladilar. Davlatning monetar siyosatidagi eng muhim amallardan biri pul emissiyasini nazorat qilish bo'lgani uchun, kriptovalyutadan voz kechish mamlakatdagi moliya-kredit tizimini va uning jahon moliya kredit tizimi bilan aloqalarini sezilarli ravishda chegaralashga va uni izdan chiqishiga olib kelishi mumkin. Respublikaga innovatsion iqtisodiyotni tezkorlik bilan rivojlantirish hamda turli xildagi innovatsion loyihalarni moliyalashtirish uchun yuqoridagi tegishli bo'limda (*5-Bo'lim. Raqamli valyutalar bozoridagi innovatsion texnologiyalar*) tavsif etilgan **ICO** (*Initial Coin Offering*) mexanizmini ham qonuniylashtirish va joriy qilish maqsadga muvofiq bo'lar edi. Bunda O'zbekistonda ishlab chiqariladigan mahsulotlar va xizmatlar bilan ta'minlangan tokenlar chiqarish va ularni ichki hamda tashqi bozorda realizatsiya qilib, yig'ilgan mablag'lar tegishli loyihalarni moliyalashtirish uchun ishlatilar edi. Loyiha amalga oshirilib bo'linganidan so'ng, tokenlar ko'rinishidagi kriptovalyutalar egalariga ularning tokenlari miqdoriga teng bo'lgan tegishi mahsulotlar yetkazilib beriladi yoki ular uchun tegishi xizmatlar amalga oshiriladi. Masalan, gipotetik **UzCotton** kriptovalyutasining (*quyida keltirilgan barcha kriptovalyuta turlari ham gipotetik mavqe'ga ega*) har biri bir kilogram paxtaga ekvivalent bo'lishi mumkin. Demak, **ICO** tashkil etuvchilar bunday tokenlarni sotib olgan huquqiy va jismoniy shaxslarga ular tokenlari miqdoriga teng bo'lgan paxta yoki tola yetkazib berish

majburiyatini o'z zimmasiga oladi. **UzGold** kriptovalyutasining bittasi bir gram oltinga ekvivalent bo'ladi, demak, loyiha amalga oshganidan so'ng, bunday tokenlar evaziga tokenlar egalari jahon birjasidagi narxlar bo'yicha O'zbekiston Respublikasida zarb qilingan oltin tangalar yoki valyuta beriladi. Agar innovatsion loyiha quyosh yoki shamol elektrostantsiyasi (*fermasi*) qurish bo'lsa, bitta **UzEnergo** kriptovalyutasi bir kilovatt energiyaga teng bo'ladi va demak elektrostantsiya ishga tushirilganidan so'ng, kriptovalyutani sotib olgan inson yoki tashkilot oldingi pastroq bo'lgan narxlarda tokenlariga mos bo'lgan elektroenergiyadan foydalanishi mumkin bo'ladi. Agar masalan, **UzKvartira** deb atalgan tokenlarning har biri bir kvadrat metr uy-joy maydoniga teng deb chiqarilgan bo'lsa, u xolda tokenlarning egalari loyiha amalga oshganidan so'ng, ushbu tokenlar miqdoriga teng bo'lgan uy-joy maydoniga egalik qila oladilar. Ya'ni ularning jalb qilingan pullariga (*kriptovalyutalar sotishdan yig'ilgan pullarga*) uy quriladi va keyin uydagi kvartiralar kriptovalyutalar egalari tokenlarga mos ravishda taqsimlanadilar. Demak, ko'pchilik insonlar uy-joyli bo'lish uchun banklardan yuqori foyizli ipoteka kreditini olish o'rniga hech qanday kredit mablag'lari jalb qilmasdan turib, uy qurayotgan kompanniyadan kriptotangalar sotib oladilar va birozdan so'ng, uy-joyli bo'ladilar. Agar ularga uy kerak bo'lmasa, kriptotangalarni ikkilamchi bozorda sotib, qo'shimcha daromad ishlab olishlari ham mumkin. Buni kriptovalyutalardan foydalanishning spekulativ usuli deb atash mumkin.

Ushbu risola kriptovalyutalarga bag'ishlangan va o'zbek tilida yozilgan birinchi kitob bo'lib, kamchiliklardan holi emas, albatta. Unda kriptologiya, kriptografiya, kriptovalyuta, uning turlari, tarqalishi, ishlatilishi, tarixi, rivojlanishi, bozorlari, birjalari, almashinuv punktlari, **ICO** lar va ularni tashkil qilish mexanizmi hamda kriptovalyutalardan foydalanilish va ularning rivojlanish tendentsiyalari bo'yicha baholi-qudrat bir qancha ma'lumotlar berilgan. Agar siz bu risoladan o'zingiz uchun kerakli bo'lgan yangi hamda foydali ma'lumotlar topa olgan bo'lsangiz va undagi ko'rsatmalardan foydalangan xolda bu qiziqarli olamga ekskurs qilmoqchi bo'lsangiz biz o'z maqsadimizga erishgan bo'lar edik. Shuni ham aytishimiz

kerakki, har qanday yangi ma'lumot, u qanchalik foydali bo'lmasin, amalda ishlatilmasa, moddiy foyda keltira olmaydi. Buni unutmang, va bilimlaringizni amalda ishlatishdan erinmang. Bunda albatta tavakkalchilik qilishga to'g'ri keladi, albatta. Ammo tavakkal qilmasangiz, hayotda hech nimaga erisha olmaysiz. Tavakkalchilik darajasini kamaytirishni usuli esa aktivlarning diversifikatsiyasi, doimiy o'qish va o'rganish, yangi texnologiyalarni bilish va tushunish, ishonchli hamkorlar topishdir. Shundagina birni ikki, ikkini esa to'rt qila olasiz.

### ***Glossariy***

**Kalit** – matnlarni hech qanday to'siqlarsiz shifrlash va deshifrlash uchun zarur bo'lgan ma'lumot

**Elektron raqamli imzo** – matnga biriltirilgan va uning kriptografik o'zgartirilishini aniqlab beradigan ma'lumot bo'lib, matn boshqa foydalanuvchi tomonidan olinganida uning haqiqiyligini va muallifini tekshirishga imkon beradi

**Kriptobardoshlilik** – kalitni bilmasdan turib, shifrlangan matnni deshifratsiya qilish imkoniyati qandayligini ko'rsatadigan kattalik

**Kriptobardoshlilik ko'rsatgichlari** – barcha mumkin bo'lgan kalitlar soni va kriptozanaliz uchun zarur bo'lgan o'rtacha vaqt

**Raqamli imzo** – qandaydir mahfiy kalit yordamida generatsiya qilingan ma'lumotlar blogi. Ochiq kalit yordamida haqiqatan ham ma'lumotlar shu mahfiy kalit yordamida generatsiya qilingani tekshiriladi

**Xesh-funktsiya yoki daydjest-funktsiya** – boshlang'ich ma'lumotning nazorat yig'idisi bo'lib (*bir tomonlama funktsiya*), ma'lumotlarning ishonchsiz aloqa kanallari orqali uzatilishini tekshirish vositasidir (*bunda ma'lumotlarning butunligi tekshiriladi*). Ma'lumot mahfiy kalit bilan shifrlangan xehs-funktsiya bilan birgalikda uzatiladi. Ma'lumotni oluvchi boshlang'ich axborotni olganidan so'ng, uning xesh-funktsiyasini aniqlaydi va uni qabul qilingan ma'lumotning xesh-funktsiyasini bilan solishtiradi va shundan so'ng tegishli qaror qabul qiladi.

**MD2, MD4, MD5 xesh-funktsiyalari** – havfsizlik tizimlaridagi eng ommabop bo'lgan xesh-funktsiyalar bo'lib, uzunligi 16 bayt bo'lgan daydjestlarni generatsiya qiladilar.

**SHA-amerika standartidagi xesh-funktsiya** – **MD4** xesh-funktsiyaning adaptatsiya qilingan varianti hisoblanadi. Uning daydjesti uzunligi 20 baytdir.

**MDC2 va MDC4 xesh-funktsiyalar** – IBM kompaniyasi tomonidan foydalaniladigan bir tomonlama xesh-funktsiyalar bo'lib, ular **DES** shifrlash algoritmiga asoslangan.

**Pul** – biror bir alohida mamlakatning, yoki kelishuv asosida bir nechta davlatlarning tovar va xizmatlar oldi-sottisi uchun umumiy ekvivalent sifatida qabul qilinadigan valyutasi bo'lib, u qog'oz, metal yoki elektron ko'rinishda bugungi kun iqtisodiyotida amal qiladi.

**RSA algoritmi** - (*Random Signature Algorithm*) – Asimmetrik shifrlash algoritmi

**DSA algoritmi** - (*Digital Signature Algorithm*) elektron raqamli imzo uchun AQSH standarti (*Digital Signature Standart – DSS*)

**DSS** - Digital Signature Standart

**Xesh** – istalgan uzunlikdagi ma'lumotlar massividan oldindan aniqlangan uzunlikdagi qandaydir qiymat olish uchun amalga oshiriladigan o'zgartirishdir

**Xesh funktsiya** - katta hajmdagi (*masalan, 125 megabaytli ma'lumot*) fayllarga elektron raqamli imzo qo'yishdan avval undan xesh-funktsiya hisoblanadi va shundan so'ng uning qiymatiga elektron raqamli imzoni hisoblaydilar

**Tranzaktsiya** – deganda an'anaviy yoki noan'anaviy pul o'tkazishlar amaliyoti tushuniladi.

**Bitkoin kriptovalyutasi** – bu o'zaro ishonchga emas, balki kriptografik kodlash tizimiga asoslangan, o'zaro hech qanday vositachilarsiz (*bank yoki*

*boshqacha moliyaviy uskunalarsiz*) to'lovlarni bevosita ishtirokchilar orasida amalga oshirilishini ta'minlovchi to'lov tizimi valyutasining bir turidir.

**Kriptologiya** – kriptografik usullarning qo'llanilishini anglatib, kriptografiya va kriptozanalizga bo'linadi

**Kriptografiya** – informatsiyani himoyalash uchun uni o'zgartirish usullarini o'rganishning matematik metodlarini anglatadi

**Kriptozanaliz** - kalitlarni bilmasdan turib, informatsiyani rasshifrovka qilish usullarni o'rganishni anglatadi.

**Kriptografiyaning asosiy bo'limlari** – simmetrik kriptotizimlar, ochiq kalitli kriptotizimlar, elektron imzoli tizimlar va kalitlarni boshqarish

**Alfavit** – belgili informatsiyani kodlashtirish uchun ishlatiladigan chegaralangan to'plam

**Matn** – alfavit elementlarining tartiblangan bo'lagi

**Shifrlash** – boshlang'ich ochiq matnni shifrlangan matnga aylantirish jarayoni

**Deshifrlash** – shifrlashga teskari jarayon bo'lib, unda ma'lum kalit asosida shifrlangan matn boshlang'ich matnga aylantiriladi

**Bitkoin pitstsa kuni (*Bitcoin Pizza Day*)** – 2010 yilda aynan shu kuni chexiyalik dasturchi Lazlo Xanesh bitkoinga dastlabki haqiqiy savdoni amalga oshirgan, ya'ni, o'z o'rtog'iga 10 ming bitkoin o'tkazib bergan va o'rtog'i o'z navbatida unga *Papa John's* restoranidan ikkita pitstsa buyurtma qilgan. O'sha vaqtda bir bitkoin 0,003 **AQSH** dollariga teng bo'lgan va ikkita pitstsaning narxi esa 30 dollar bo'lgan.

**BTC – Bitkoin** – kriptovalyutalarning eng asosiy turi

**BCH - BitcoinCash** – bitkoinning egizagi

**Ethereum** - kapitalizatsiya bo'yicha ikkinchi o'rinda turuvchi kriptovalyuta turi

**Hamyon** yoki **Koshelek** yoki **Wallet** - mablag'larni tarmoqning bir qismi bo'lgan **hamyon** faylida saqlanishi

**Litecoin (Laytkoyn)** - kriptovalyuta dunyodagi ommalashgan kriptovalyutalar turlaridan biri hisoblanadi



**ICO** – kriptovalyuta tanga-tokenlarini birlamchi joylashtirish — *Initial Coin Offering*

**Blokcheyn** — raqamli kriptovalyutalar haqidagi ma'lumotlarni saqlash uchun foydalaniladigan komp'yuter tarmoqlariaro taqsimlangan reyestr, ya'ni, biri biri bilan internet orqali bog'langan ko'plab kompyuterlarda bir vaqtning o'zida saqlanuvchi taqsimlangan ma'lumotlar bazasi

**Hyperledger - Linux Foundation** бошчилик киладиган блокчейн-консорциум

**Bitcoin, laytkoin, token** – electron valyuta turlari – ya'ni, electron kriptovalyutalar

**Kriptovalyuta birjalari** – electron raqamli pullar – kriptovalyutalar bo'yicha pul o'tkazmalarini amalga oshiradigan birjalar

**Token** yoki **Tanga** - Blokcheynlar bilan ishlovchi turli loyihalar chiqaradigan boshqa turdagi kriptovalyuta.

«**Mayning**» – bu kompyuter tizimlarining hisoblash quvvatlarini kriptovalyutaning tranzaksiyalari zanjirini xosil qilish uchun ishlatilish jarayonidir. Kriptovalyutalarning emissiyasi xuddi shu **mayning** (*kriptovalyuta tangalarini qidirib toppish, qo'lga kiritish*) tamoili asosida amalga oshiriladi. Boshqacha qilib tushuntirganda, mayning (*mayning*) – shirlangan dasturiy kodni raqamlar varuatsiyasini tanlash yordamida topishga erishishdir. Mayning jarayoni blokcheynga kiritiladigan ma'lumotlar bloki zanjirini hisoblab topishdir, deyishimiz ham mumkin. Tizimning barcha talablarga javob beradigan yangi ma'lumotlar blogini hisoblab topish va uni tashkil etgani uchun maining bilan shug'ullanuvchi inson – mayner bir qancha kriptovalyutalar birligi ko'rinishidagi mukofotlanuvni oladi. Ushbu kriptovalyuta esa o'z navbatida, istalgan turdagi valyutaga (*dollar, evro, iyen, von va boshqalarga*) konvertatsiya qilinib olinishi mumkin. Shuni ham hisobga olish kerakki, har bir kriptovalyuta blogini hosil qilishga bir vaqtning o'zida jahon miqyosida bir qancha maynerlar kurash olib boradilar. Komp'yuteri eng tez va kuchli bo'lgan maynergina bu kurashda yutib chiqadi va tegishli mukofitni qo'lga kiritadi. Mayning jarayonini sodda xolda

AYUPOV R.H., KABULOV V.K.

komp'yuter tomonidan murakkab masalalarni hal qilish jarayoni deb tushuntirish ham mumkin. Har bir masalani yechganlik uchun mayner elektron pullarga ekvivalent bo'lgan ma'lumotlar paketini oladi. Ushbu bloklar asta sekin yig'ilib, bir butun dasturiy kodga aylanadilar va ularning ma'lum bir guruhi kriptovalyutaning ma'lum bir birligini hosil qiladi.

**Maining fermalari** – Mayning qilish maqsadida katta inshootlardan foydalangan xolda doimiy ravishda ishlab turuvchi yirik serverlardan iborat komp'yuter tizimlari.

**Maynerlar** - bir vaqtning o'zida yangi kriptopullarni topadilar va kriptovalyutaning barcha mumkin bo'lgan turlardagi tranzaksiyalarini amalga oshiradilar

**Pirring arxitekturas**i - bunday tarmoq arxitekturas i bir huquqqa ega bo'lgan mijoz dasturlaridan iborat bo'ladi.

**Kritovalyuta tangalarini emissiya qilish cheklovi** – jami 21 million **BTC** (*bitkoin tangasi – token*) chiqariladi

**Anonimlik** - pul mablag'lariga anonim jihatdan (*egasi ko'rsatilmagan xolda*) egalik qilish va ulardan foydalanishning anonimligi (*bunga tranzaksiyalar ham kiradi*)

**Markazlashmagan tizim** – bunday tizimda har bir ishtirokchi teng huquq va imkoniyatlarga ega bo'lishi ko'zda tutilgan

**Fiat pullar** - nominal qiymati real qiymatidan katta farq qiladigan pullar

**SHA-256** - xeshlashtirish usuli yoki algoritmi

**Z.com** - yapon kriptovalyuta birjasi

**CryptA Capital** – kriptovalyutalar investitsion portfeli tuzishga imkon beradigan **Alpari** halqaro moliyaviy kompaniyasi platformasi

**alpari.com** – Xalqaro miqyosdagi moliyaviy kompaniya sayti

**Xesh** – istalgan uzunlikdagi ma'lumotlar massividan oldindan aniqlangan uzunlikdagi qandaydir qiymat olish uchun amalga oshiriladigan o'zgartirishdir

**shifrovkachilar** - ma'lumotlarni shifrovka qilish uchun bu sohaga mahsus o'qitilgan insonlar

**Konfidentsiallik** – bu informatsiyaning saqlanishida va uzatilishida ma'lumotlarni ruhsat berilmagan o'qishdan himoya qilishdir. Bu shifrlash orqali amalga oshiriladi;

**Ma'lumotlardan foydalanishning nazorati** – informatsiyadan faqatgina ruxsat berilgan insonlar foydalana olishi kerak;

**Autentifikatsiya** – ma'lumot uzatuvchi kimligini aniq bilish imkoniyati. Buni electron raqamli imzo va sertifikat amalga oshirib beradi;

**Butunlilik** – informatsiyaning saqlanish va uzatilish jarayonida ruxsatsiz o'zgartirila olinmasligi. Bu talab electron raqamli imzo va imitohimoya orqali bajariladi;

**kalit** - komp'yuter texnikasi ishlatilganda kalit bu son yoki sonlar ketma-ketligidir

**Shifrlash algoritmlari** - bir necha yillar davomida yaratiladigan va sozlanadigan matematik funktsiyalardir

**RC4 va DES (3DES, DESx)** - ommabop shifrlash algoritmlari

**IDEA shifrlash algoritmi** - konfidentsal bo'lib, **AQSH** xukumati tomonidan ishlab chiqilgan va uning qandayligi hech kimga hach qachon ma'lum qilinmaydi

**RC4 (Rivest cipher 4)** va **DES (Data Encryption Standart)** - simmetrik shifrlashning eng ko'p ishlatiladigan protokoli 1976 yilda AQSH davlati tomonidan kritik bo'lmagan informatsion massivlarini himoya qilish uchun ishlatishga mo'ljallangan kriptografik standart

**HSM – Hardware Storage Module** - havfsizlik tizimlarining ko'pchilik turlarida kalitlar saqlashning apparat modullarida yoki smart kartalarda saqlanadi

**Ochiq kalitlar texnologiyasi** - Shifrlashning ikkinchi usuli hisoblanib, uni asimmetrik kriptografiya deb ham atashadi. Ushbu usuldan

foydalanganda ikkita kalitdan foydalaniladi: ochiq (*ommaviy*) va yopiq (*mahfiy*) kalitlar

**“shaffof” shifrlash dasturlari** - o'z komp'yuteringizdagi ma'lumotlarni shifrlab qo'yishning bir necha xil usullari mavjud bo'lib, ularning ichidan foydalanuvchi uchun bilinmaydigan “shaffof” shifrlash dasturlaridan foydalanish tavsiya etiladi. Bunday programmalar komp'uterning mantiqiy disklarini shifrlash uchun ishlatiladi.

**RSA** (*Random Signature Algorithm*) - asimmetrik shifrlash algoritmi.

**DSA algoritmi** - (*Digital Signature Algorithm*) - 1981 yilda yaratigan bo'lib, electron raqamli imzo uchun **AQSH** standarti (*Digital Signature Standart – DSS*) sifatida ishlatiladi.

**Xesh** – istalgan uzunlikdagi ma'lumotlar massividan oldindan aniqlangan uzunlikdagi qandaydir qiymat olish uchun amalga oshiriladigan o'zgartirishdir

**FOCT 3 34.11-94** - Rossiyada qo'llaniladigan standart xesh-kattalikni aniqlash standarti (*yoki xesh-funktsiya*) bo'lib, u 32 bayt kattalikda hisoblanadi.

**MDx (Message Digest)** – chet mamlakatlarda eng ko'p tarqalgan xeshlashtirish algoritmlari oilasi. Masalan, **MD5 Microsoft Windows** ning oxirgi versiyalarida foydalanuvchi parolini 16 baytli songa aylantirish uchun foydalaniladi.

**SHA-1 (Secure Hash Algorithm)** – kirish ma'lumotlarini 20 baytli xesh-miqdorga aylantirishning hisoblash algoritmi. Bu algoritm ham jahon miqyosida keng tarqalgan bo'lib, ko'pincha ma'lumotlarni himoyalashning tarmoq protokollarida ishlatiladi

**PKI - Public Key Infrastructure** - ochiq kalitlarning infratuzilmasi

**Sertifikatsiya markazi, registratsiya markazi va tarmoq ma'lumotnomasi** - ochiq kalitlar infratuzilmasi tarkibiga kiradigan tashkiliy tizimlar

**RSA Keon** - elektron raqamli imzolarni qayd qilish markazi foydalanadigan dasturiy-texnik kompleks

**CGMiner** – Ushbu dastur virtual pullarni topish (*mayining qilish*) bo'yicha ishlaydigan professionallar uchun mo'ljallangan algoritm.

**Diablo Miner** – Hozirgi vaqtda mavjud bo'lgan barcha operatsion tizimlarda bir xilda ishlay oladigan va kriptovalyutalarni mayning qilishga mo'ljallangan sayt

**Ufasoft Miner** – Mayning qilishning ushbu dasturi ishchi ko'rsatgichlarini sozlash mumkinligi tufayli mutaxassislar orasida ancha ommabop hisoblanadi

**BFG Miner** – Mayningning bu dasturda esa foydalanuvchilar qo'l rejimida pu'llarni sozlashi va boshqa ishlarni amalga oshirishi mumkin

**Phoenix** – Mayningning ushbu dasturi juda samarador ishlaydigan dasturlar qatoriga kiradi va mayning ish unumdorligini 20% ga ko'tarish imkonini beradi

**Solo-mayning jarayoni** - virtual pullarni mustaqil ravishda topishini anglatadi

**Pu'l-mayning** – bir qancha kichik maynerlar o'zlarining resurslarini bir joyga yiqqan xolda kriptovalyuta mayningi bilan shug'ullanishini anglatadi

**RDP-mayning** – Bulutli deb nomlangan texnologiyalarning keng miqyosda ishlatilishi tufayli kriptovalyutalar topishning (*mayningning*) kollektivizmga asoslangan bir turi

**hardfork** - kriptovalyuta dastur kodining yangilanishi

**XMine, Multi-Coin, AroMine, BiteMiner** va **Bit-Lite** - Internetda ajratilgan qandaydir miqdordagi kriptobonus tufayli kriptovalyutalar mayningini boshlang'ich pul mablag'lari sarf qilmasdan turib boshlashga imkon beradigan xizmatlar.

**SpectroCoin** - kriptovalyutalar birjasi

**Sidechain** - biror-bir kanalning yoki qurilmaning qandaydir ko'rsatgichlarini boshqa bir qurilma yoki signal vositasida boshqarish usuli

**Smart-kontrakt** - blokcheyn texnologiyasi asosida kontraktlar tuzish va uni bardavom etishga mo'ljallangan komp'yuter dasturi

**Virtual valyuta** – narxni belgilash vositasi bo'lib, u bilan raqamli ko'rinishda savdo qilish mumkin. Virtual valyuta almashinuv vositasi, hisob pul birligi va/yoki qiymatni saqlash vositasi sifatida amal qilishi mumkin. Ammo u hozircha qonuniy to'lov vositasi statusiga ega emas.

**fork (англ. fork – «вилка»)** – kriptovalyuta asosida yotgan dasturiy kodning o'zgarishi yoki modifikatsiyalashuvi yohud blokchein tizimining tamolillari o'zgarishi bo'lib, ularga mos ravishda transaksiyalar haqidagi ma'lumot bloklari hosil qilinadi va ular global tarmoqqa qo'shiladi

**Softfork (yumshoq fork, «Мягкий»)** kriptovalyuta yaratish texnologiyasiga minimal aralashuv bo'lib, aktiv uchun jiddiy ta'sir qilmaydi;

**Xardfork (qattiq fork, «Жесткий»)** – kriptovalyuta kodining tubdan ozgartirilishi tushunilib, bunda uning ishlash jarayoniga ham ta'sir qilinadi, Natijada transaksiyalar hosil qilinish va maining printsiplari ham o'zgarishi mumkin.

**Efirium yoki Efir** – bu nafaqat kriptovalyuta, balki to'laqonli platforma bo'lib, uning yordamida istalgan aktivlar (*valyuta, qimmatli qog'ozlar va boshqalar*) bilan ish olib borish mumkin. Uning imkoniyatlari blokcheynga yangicha yondoshuv natijasida bitkoin potentsialidan ham kattaroqdir. Uni aqlli kontraktlar asosida ishlaydigan markazlashmagan virtual mashina deb tushunish ham mumkin.

**STForex** – STForex asosida ishlaydigan savdo terminali AQSH dollari, evro va rubl asosida Bitcoin, Dashcoin, Ethereum, Litecoin, Namecoin, Peercoin lar bilan ishlay oladi. Unda osongina bitkoinga efirium sotib olishingiz mumkin.

**Blokcheyn** – ma'lumotlar bloklarining uzluksiz zanjiri, ya'ni bir butun ma'lumotlar bazasi bo'lib, unda kriptovalyutalar bilan amalga oshirilgan barcha ma'lumotlar saqlanadi. Uni kim, qachon va qancha operatsiyalar amalga oshirganini ko'rsatib turadigan katta hisob-kitob jurnali deb tasavvur qilish ham mumkin.

**Anonimlilik** – blokcheyn ishtirokchisining elektron hamyoni telefon raqamiga ham, nomga ham, manzilga ham bog'liq bo'lmaydi. Unda faqatgina blokcheynda qayd qilingan hamyon nomeri va unga bog'liq bo'lgan hamda egasi biladigan parol bo'ladi holos. Blokcheynning shaffofligidan foydalangan xolda transaktsiyalar haqidagi ma'lumotlarni ko'rganda hamyonlar qancha bitkoin olganini bilish mumkin, uning egasini aniqlab bo'lmaydi (*albatta uning o'zi buni aytmasa*). Agarda kriptovalyuta egasi hamyon nomeri yoki parolni yo'qotib qo'ysa, u xolda uning o'zi ham tizimga kira olmaydi.

**Havfsizlik** – blokcheynga mustaqil ravishda hech kim o'zgartirish kirita olmasligi tufayli, kriptovalyutani ham qalbakilashtirish mumkin emas.

### ***Adabiyotlar ruyhati***

1. **Натаниэль Поннер.** Цифровое Золото. Невероятная история биткойна или о том, как идеалисты и бизнесмены изобретают деньги заново, 2016, 350 стр.
2. **Евгений Филиппов.** Криптовалюта от А до Я. ST FOREX, 2017
3. **Don Tapscott, Alex Tapscott.** Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World, 2016, 324 pages.
4. **Paul Vigna, Michael Casey.** The Age of Cryptocurrency: How Bitcoin and the Blockchain Are Challenging the Global Economic Order. 2015, 384 pages.
5. **Melanie Swan.** Blockchain: Blueprint for a New Economy, 2015, 152 pages.
6. **Phil Champagne.** The Book of Satoshi: The Collected Writings of Bitcoin Creator Satoshi Nakamoto»; 396 стр.; 2014 г.
7. **Jeremy Clark.** Bitcoin, blockchain, cryptocurrency, cryptology (A detailed and technical study of Bitcoin, blockchain, cryptocurrency, and cryptology);; 499 стр.; 2016
8. **Jacob William.** Blockchain: The Simple Guide To Everything You Need To Know. 2016, 69 pages.
9. **www.alpari.com** – xalqaro miqyosdagi moliyaviy kompaniya sayti
10. **www.coinspot.io/analysis** – veb sayti
11. **www.bitnovosti.com** – veb sayti
12. **www.24paybank.com/news**– veb sayti

13. [http://karpilovskyy.com/?utm\\_source=google&utm\\_medium=cpc&utm\\_campaign=search](http://karpilovskyy.com/?utm_source=google&utm_medium=cpc&utm_campaign=search) – kriptovalyuta bozorlari, kriptovalyutalar va blokcheynlar o'yicha naster klass.
14. **Z.com** - yapon kriptovalyuta birjasi
15. <https://bitcoin.org> – Bitkoinning rasmiy sayti
16. <https://ru.wikipedia.org/wiki/> - Vikipediadagi sahifa
17. [https://bitcoin.org/files/bitcoin-paper/bitcoin\\_ru.pdf](https://bitcoin.org/files/bitcoin-paper/bitcoin_ru.pdf) - Satoshi Nakamotoning original maqolasi
18. <http://bitnovosti.com> – Bitkoin yangiliklari
19. <http://www.bitnovosti.tv> – kriptovalyutalar haqida onlayn video
20. <http://blockchain.community> – Rossiyaning blokcheyn jamiyati
21. <http://bitcoinembassy.ru> – Mockvadagi blokcheyn-elchixona
22. <http://ru.newsbtc.com> – Bitkoin va blokcheyn yangiliklari
23. <https://forum.bits.media> – rus tilidagi bitkoin forum
24. <https://www.youtube.com/watch?v=Aybt-Uzb4kk> – Kriptovalyutalar. Raqamli asrning oltinlari – hujjatli film

***Ravshan Hamdamovich Ayupov,***

***Anvar Vasilovich Kabulov.***

**Kriptografiya va kriptovalyutalar. Toshkent: Mirzo Ulug'bek nomidagi Uzbekiston Milliy Universiteti, 2018, 144 bet.**



