RƏQƏMSAL İQTİSADİYYAT, BLOKÇEYN, KRİPTOVALYUTA

Sabit Bağırov

13 Dekabr, 2017

Təqdimatın içindəkiləri:

- Rəqəmsal iqtisadiyyat;
- BLOKÇEYN;
- KRİPTOVALYUTA;
- BİTKOİN;
- HƏŞləmə;
- Mayninq;
- Smartkontrakt;
- İCO;
- TOKEN

Rəqəmsal iqtisadiyyat

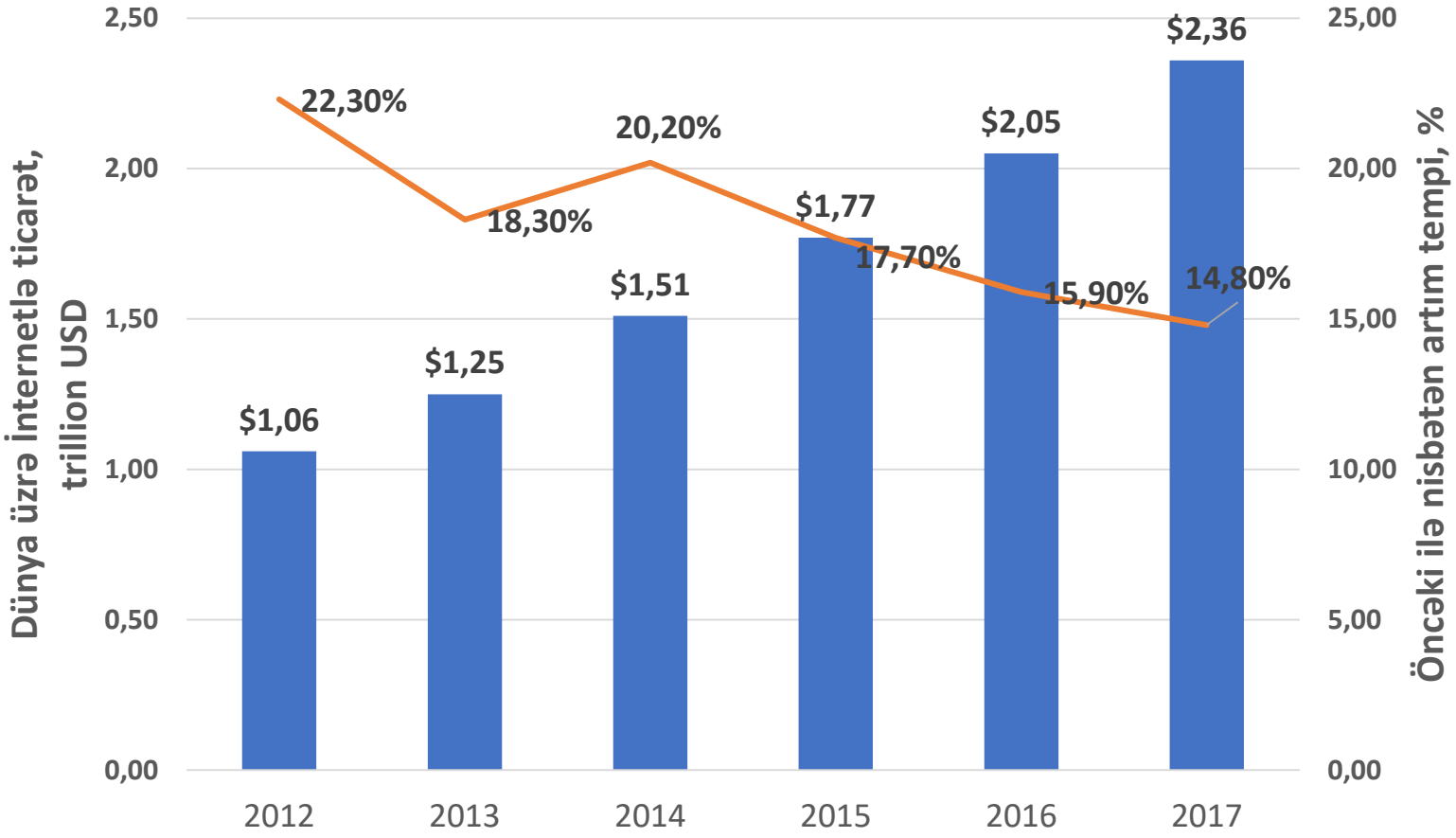
Wikipedia-ya əsasən: «Elektron (rəqəmsal, veb, internet) iqtisadiyyat – rəqəmsal texnologiyalara əsaslanan iqtisadi fəaliyyətdir. Söhbət proqram təminatı məhsullarının tərtibatı və satışından daha çox elektron biznesin və elektron ticarətin istehsal etdiyi elektron mallar və xidmətlərdən gedir. Elektron xidmətlərə və mallara görə ödənişlər daha çox halda elektron pullarla həyata keçirilir».

Elektron iqtisadiyyatın miqyasını qiymətləndirmək cəhdləri çətinliklərlə üzləşir. Elektron ticarəti ölçmək daha asandır.

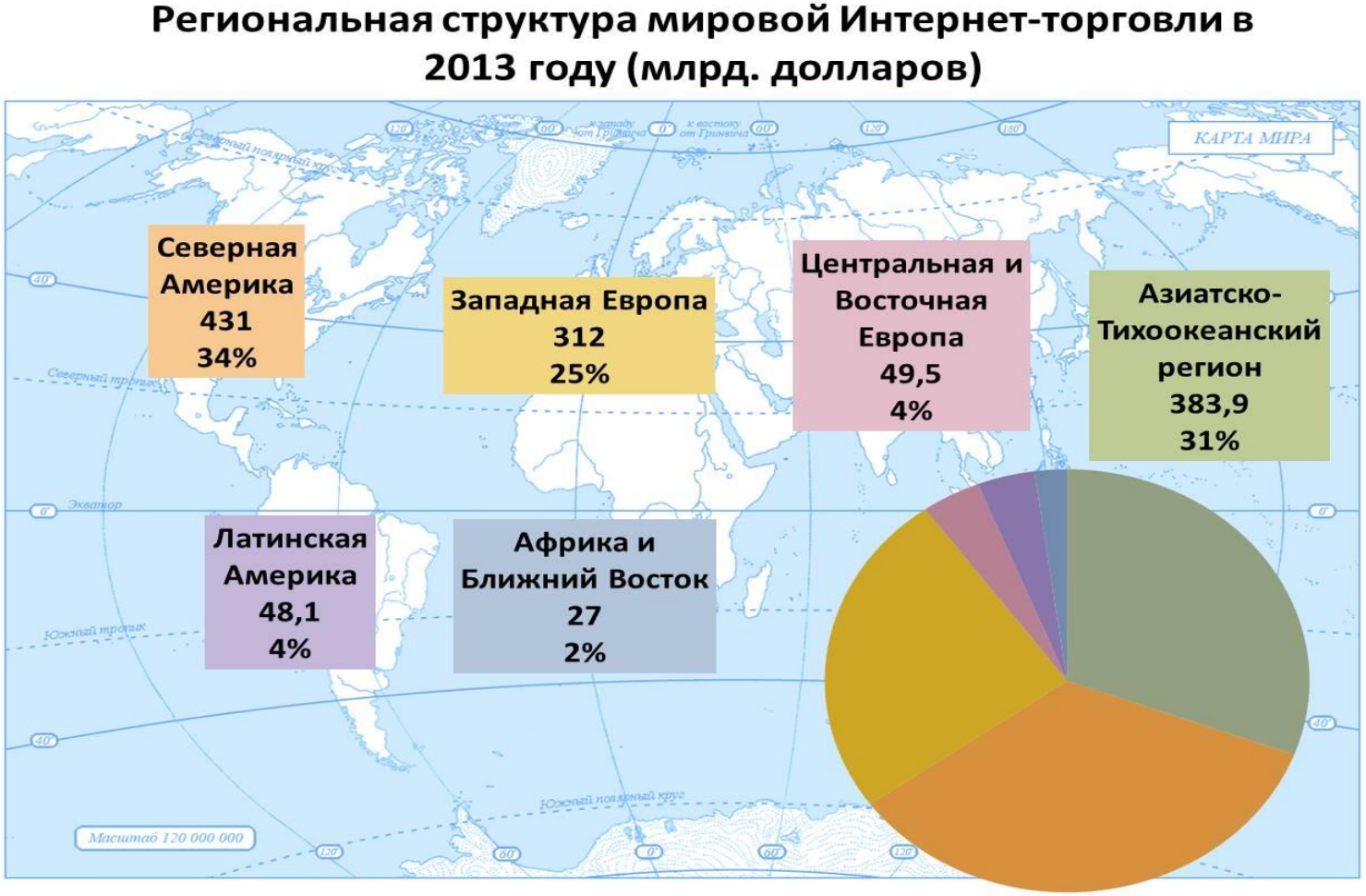
Böyük Britaniyanın İnternet iqtisadiyyatı 2012-ci ildə ÜDM-in 8.3%, 2-16-cı ildə isə 12%-nə bərabər olmuşdur.

Dünya üzrə İnternet-dükkanlardan ticarətin həcmi

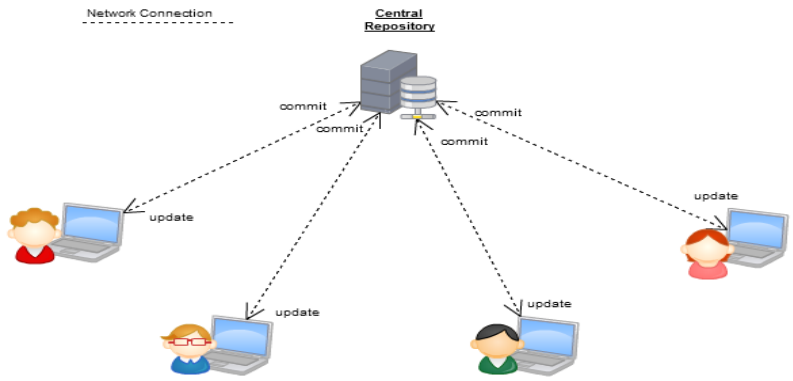
(https://www.shopolog.ru/metodichka/analytics/statistika-internet-torgovli-v-stranakh-mira/)



Dünya İnternet-ticarətin regionlar üzrə həcmləri, mlrd.USD

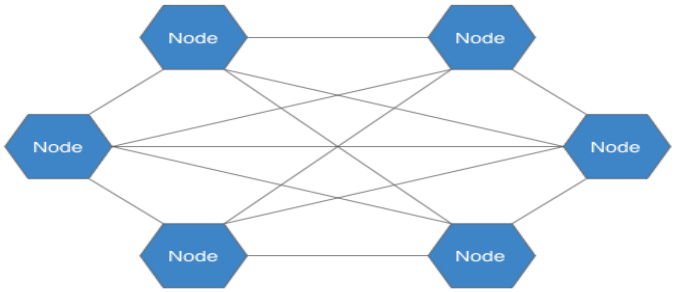


Mərkəzli və mərkəzsiz sistemlər.



Üstünlük: İnzibatçılığın, təkmilləşdirmənin, miqyasın artırılması sadəliyi

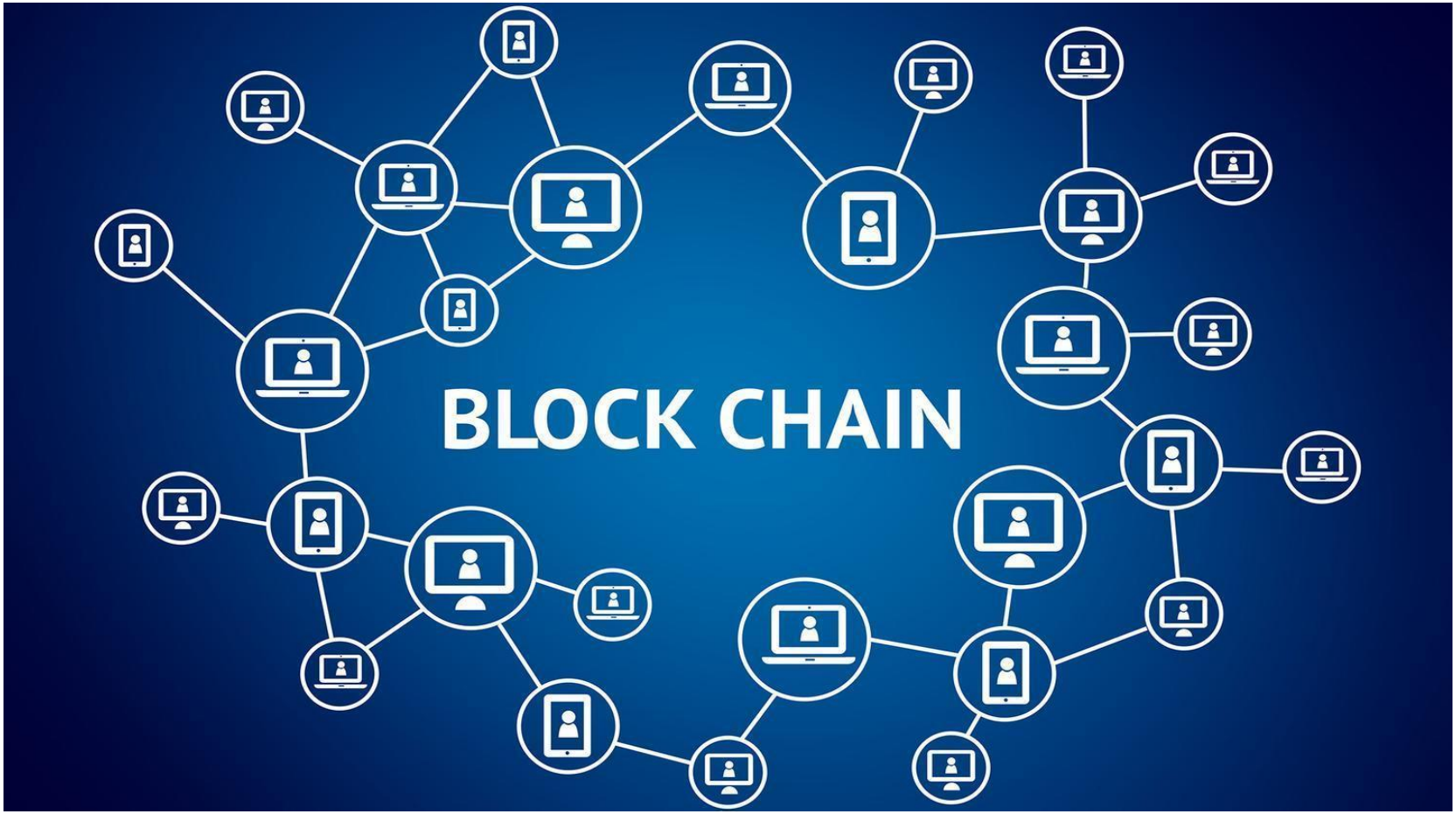
Zəif cəhədi: Kənar müdaxilə təhlükəsi



Üstünlük: Dayanıqlılıq. Kənar müdaxilədən qorunma

Zəif cəhədi: Təkmilləşdirmənin və miqyasın artırılması çətinlikləri, inhisarçılıq təhlükəsi, sosial konsensus tələbi

Blockchain (Blokçeyn) - Verilərin paylanmış şəkildə saxlanması və işlənməsi texnologisidir.



Blokçeynin əsasındakı prinsiplər

- **Verilərin paylaşması**. Verilər bazası hər kəsə və tam həcimdə çatımlıdır. Verilər bazası mərkəzləşdirilmiş idarə edilmir (PİRİNQ şəbəkəsi);
- **Bərabər hüquqluluq**. İştiakçılar arasında heç bir ierarxiya yoxdur;
- **Şəffaflıq**. Hər bir əməliyyat hər iştirakçıya açıqdır;
- **Təhlükəsizlik**. Verilər bazası təiştirakçılarda təkrarlanır.

Blokçeyn məvhumu məhz Bitkoin konsepsiyasından sonra istifadə edilməyə başladı.

Blokçeyn iqtisadiyyatının 7 prinsipi

Yeni iqtisadiyyat mühəndisliyə, kompyüter sistemlərinə, riyaziyata, kriptoqrafik üsullara və davranış iqtisadiyyatına əsaslanır

1. Şəbəkə bütövlüyü. İnam və etimad sistemin daxilində formalaşır, kənardan diktə edilmir;
2. İşlərin paylaşması. Heç kəs, heç bir qurum sistemi söndürə bilməz;
3. Dəyər stimuldur;
4. Təhlükəsizlik;
5. Məxfilik (Private anlamında);
6. Hüquqların təmin edilməsi;
7. İştirakçılıq. Hər kəsin marağına işləyən iqtisadiyyat daha yaxşı nəticələr verir.

Blokçeynin tədbiqi

1. Müxtəlif sahələrdə istifadənin mümkünlüyü söylənilir (torpaq reyestri, notariuslar, seçkilər, səhiyyə, daşıma və s.);
2. Bu günə blokçeynin əsas tədbiq sahəsi kriptovalyutalardır;
3. Blokçeinin əsas mənfi cəhəti – böyük həcmdə elektrik enerjisi tələb edir;
4. Açıq və bağlı blokçeynlər ola bilər;
5. Tədbiqi gecikdirən əsas amillər:
   - Qanunvericiliklə hələ ki tənzimlənməməsi;
   - Hökumətlərin şübhə ilə yanaşması;
   - Bank sektorunun ciddi ehtiyatlanması və s.

Nəhənglərin Blokçeyn çalışmaları

JPMorgan, Wells Fargo, State Street, SWIFT, Cisco, Accenture, London Stock Exchange, Mitsubishi UFJ Financial kompaniyalar qrupu unifi blokçeyn standart üzrə proqram kodu üzrə səylərini birləşdirərək müvafiq işlərə başlamışlar

Kriptovalyutalar

- Rəqəmsal (elektron) valyutanın növüdür. Yaradılması və nəzarət kriptoqrafik üsullara əsaslanır;
- Kriptovalyutaların işlədilməsi BLOKÇEYN texnolojisinə əsaslanır;
- Kriptovalyutaların hüquqi statusu müzakirə edilir;
- Kriptovalyuta məvhumu ilk dəfə 2011 ildə Forbes jurnalında istifadə edilib (Bitkoinə həsr edilməş məqalədə);
- Kriptovalyutalara xas olan əsas cəhəd nə daxili nə kənar administratorun olmamasıdır. Dövlət qurumları, banklar, məhkəmələr və s. Kriptovalyutalardakı tranzaksiyalara təsir edə bilməzlər;
- Bu günə 1271 kriptovalyuta mövcuddur, https://coinmarketcap.com/all/views/all/ ;
- Kriptovalyuta qəbul edən şirkətlər (misal olaraq): Microsoft, PayPal, Intuit, Jeep, Overstock.com, DISH Network, WebMoney, ……

Pulun funksiyaları

- Pulun dəyər ölçüsü olması funksiyası .
- Pulun tədavül vasitəsi funksiyası
- Pulun yığım funksiyası.
- Pulun tədiyyə vasitəsi funksiyası.
- Dünya pulu funksiyası

Kommersiya banklarının başlıca funksiyaları bunlardır:

- Müştərilərinin pullarının saxlanması;
- kreditləşdirmə;
- ödəniş və pul köçürmələrinin həyata keçirilməsi;
- konsultasiya, iqtisadi və maliyyə sahəsinə dair informasiya təchizatı.

Kriptovalyutaların inkişafında mühüm tarixlər:

1982 – Bizans qeneralları məsələsinin Lesli Lamport tərəfindən səlis riyazi həlli;

1989 – Devid Çaum tərəfindən ikili xərclər probleminin kriptoqrafik üsullarla həlli;

2005 – Nik Sabo tərəfindən kriptoqrafik üsullara və paylanmış verilər bazasına əsaslanan BitGold sistemi təklif edilir;

2008 – Satoşi Nakamotonun məqaləsində Bitkoin sistemi təqdim edilir;

2009 – İlk Bitcoin blokçeninin yaradılması;

2011 – 1 Bitkoin = 1 USD. Həmin ildə Bitkoina alternativ digər kriptovalyuta Litecoin təklif edilir;

2013 – 1 Bitkoin = 1 unsiya qızıl;

2014 – Bitkoin dövriyyəsi Western Union dövriyyəsini üstələyir;

2015 – Ethereum təqdim edilir;

2017, 13 dekabr, saat 00.30 – Bitkoinin kapitalizasiyası = 294 mlrd, 1 Bitkoin = $17565

Aktivlərin qrupları

- Daşınmaz əmlak: $191 trillion
- Borclar bazarları: $94 trillion
- Səhmlər: $55 trillion
- Kənd təsərrüfatı torpaqları: $29 trillion
- Qızıl: $6 trillion
- Kriptovalyuta: $0,3 trillion

Bitkoin

- Yaradıcısı Satoşi Nakamoto sayılır (şəxsin və ya qrupun adı);
- Virtual pul vahididir;
- Fiat pullar kimi ödəniş, yığım, tədavül, tədarük funksiyalarını yerinə yetirə bilir;
- Fiat pullardan fərqləri: 1) daha böyük səviyyədə dünyavilik; 2) mərkəzləşdirilmiş emissiya olunmur; 3) bütün ödənişlər banlarsız aparılır; 4) məzənnəsi yalnız pul bazarlarında müəyyənləşir;
- İnamsızlıq problemini həll edir;
- “proof of work” (işin sübutu) prinsipinə əsaslanır;
- «Ovlanır» - hasil edilir. Bu prosesə MAYNİNQ deyilir;
- Hər bir tranzaksiyalar blokunun bağlanmasına görə mayner-ovçu müəyyən sayda bitkoin qazanır (ilk dörd ildə 50 bitkoin. Təxminən 10 dəqiqədə bir blok bağlanır. 4 ildə - 210240 blok bağlanır. Cəmi blokçeyndə blokların sayı 6930000 blok olacaq);
- «Ovlayanlar» - «mədənçilərdir» (mayninqçilər) adlanır;
- «Ovlama» xüsusi proqram sistemi vasitəsi ilə həyata keçirilir. Proqram sistemi pulsuz əldə edilə bilər.

Mayninq – Mədənçilik

- Krptovalyutaların əksəriyyəti «Ovlanır» - hasil edilir. Bu prosesə MAYNİNQ (Mədənçilik) deyilir;
- Hər bir tranzaksiyalar blokunun bağlanmasına görə mayner-ovçu müəyyən sayda bitkoin qazanır (ilk dörd ildə 50 bitkoin. Təxminən 10 dəqiqədə bir blok bağlanır. 4 ildə - 210240 blok bağlanır. Cəmi blokçeyndə blokların sayı 6930000 blok olacaq);
- «Ovlayanlar» - «mədənçilərdir» (mayninqçilər) adlanır;
- «Ovlama» xüsusi proqram sistemi vasitəsi ilə həyata keçirilir. Proqram sistemi pulsuz əldə edilə bilər.
- Bulud ovlama: www.hashflare.io

Bitkoin

- Mayninqçilər bitkoini öz və ya başqalarının kompyüterlərində ovlaya bilərlər;
- Mayning: 1) PC-də; 2) ASİC-də (xüsusi inteqral sxem); 3) Rig farm-da aparıla bilər. https://www.buybitcoinworldwide.com/mining/hardware/
- Mayninqçilər zəhmətlərinin əvəzi olaraq bitkoinlər qazanır;
- Mayning az olmayan miqdarda elektrik enerjisi istifadə edir. Ekspertlərin hesablamalarına görə bu gün dünya üzrə mayninqə sərf olunan elektrik enerjisi İrlandiyanın sərfini aşıb. https://www.youtube.com/watch?v=0PSYJENUcNw
- Cəmi 21 mln bitkoin ovlana bilər;
- Bir Bitkoin 100 000 000 satoşiyə bölünür;
- Bitcion volotildir

Bitkoinin əsas alqoritmik xüsusiyyətləri

- Tranzaksiyalar iki açarla qorunur: açıq və gizli;
- Məlumatları şifrələmək üçün Haş funksiyalarından istifadə edilir;
- Balans blokçeyndə qeyd edilmir. Lakin öncəki tranzaksiyalar onu müəyyənləşdirməyə imkan verir;
- Hər 10 dəqiqədən bir bütün toplanmış tranzaksiyalar cüt-cüt Haşlanır və yoxlanılır;
- Uğurlu yoxlamanın sonunda yeni blok öncəki bloklara əlavə edilir;
- Yeni bloku hazırlayan Bitkoin qazanır və əlavə digər növ qazanc;

Verilərin HƏŞ-lənməsi

- Məqsəd: böyük həcmdə olan verilər massivlərini müəyyən uzunluqda qısa təsvirə (bunlara ya HƏŞ və ya Digests/Daycest deyilir) gətirmək;
- Üsul: xüsusi riyazi alqoritmlər;
- Əsas şərtlər/tələblər:
  1) fərqli verilər massivi eyni nəticə (qısa təsvir) verməməlidir (Kolliziya). ***n*** bit uzunluqda olan HƏŞ ən azı $2^{n/2}$ halda kolliziya yaranırsa müvafiq HƏŞləmə funksiyası kriptomöhkəm hesab edilir;
  2) Geriyə dönməzlik;
  3) Verilər massivlərində lap kiçik fərq HƏŞlərin heç də kiçik fərqlənməsini verməməlidir

Həş funksiyalar

$$y = f(x)$$

Burada: x – müəyyən işarələr ardıcıllığıdır (verilər massiv);

y – funksiyaya uyğun alınan qısa təsvir (şifr);

1. Kompyüterləşmənin ilk mərhələsində əsas yoxlama üsulu Nəzarət Cəmi olub:

$$y = \sum_{i=1}^{n} x(i)$$

2. Bəzi Həş funksiyalar: DM-5, DM-6, ГОСТ Р 34.11-94**,** Sha-1, Sha-2, Sha-256, SCRYPT, ...

3. Digər növ funksiyalar

4. Haş funksiyalar böyük mətni, məsələn 500 səhifəlik kitabı 30 (və ya digər) işarədən ibarət bir sətrdə əks etdirməyə imkan verir.

HƏŞləmə nümunələri

Misal üçün, Sha-1 HƏŞləmə fünksiyası aşağıdakı mətnin:
Mənin bu gün saat 15.00-da bankla görüşüm var.
HƏŞi belədir:
CD00DF7D200340B7B80DB3C5D6D2EFC7FAB72AB1

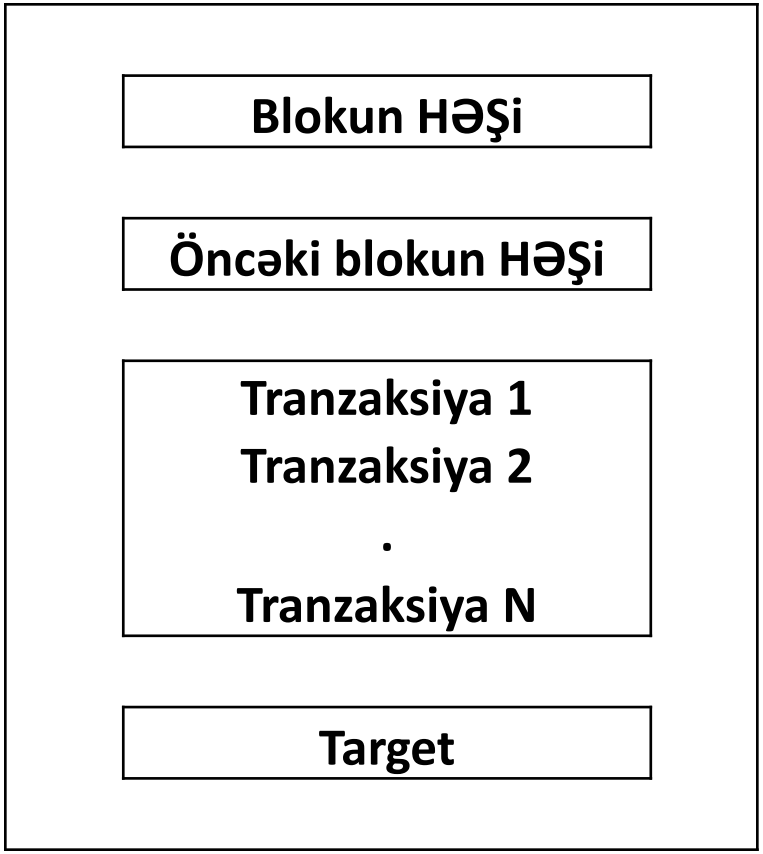
Bu mətnin:
ənin bu gün saat 15.00-da bankla görüşüm var.
HƏŞi belədir:
B56A341A77A5B11EAC6C890B79D29C7FFEE3C6A6

https://www.cryptolocker.az/decrypt

Rəqəmsal imza

- Cuzdanın şifri İki hissədən ibarətdir: açıq və bağlı açarlardan;
- Bağlı açarla sənədin (tranzaksiyanın) HƏŞ-i imzalanır;
- Açıq açarla tranzaksiyanın kimə ünvanlandığı göstərilir;
- Pul köçürülərkən alanın açıq açarı qeyd olunur;
- Hər yeni tranzaksiya üçün açar təzələnir ki, xaker ondan istifadə edə bilməsin. Mümkün ola bilən bitkoin ünvanların sayı = **1.46×10^{48} və ya 2^{160}** ;
- Bağlı açar itirildikdə onun sahibinin bütün bitkoinlər itir. Bərpa etmək praktik olaraq mümkün deyil. Qeyd edək bu itirilən bitkoinlər ümumiyyətlə dövriyyədən çıxarılır;
- İmza şifri elleptik funksiya əsasında hesablanır;

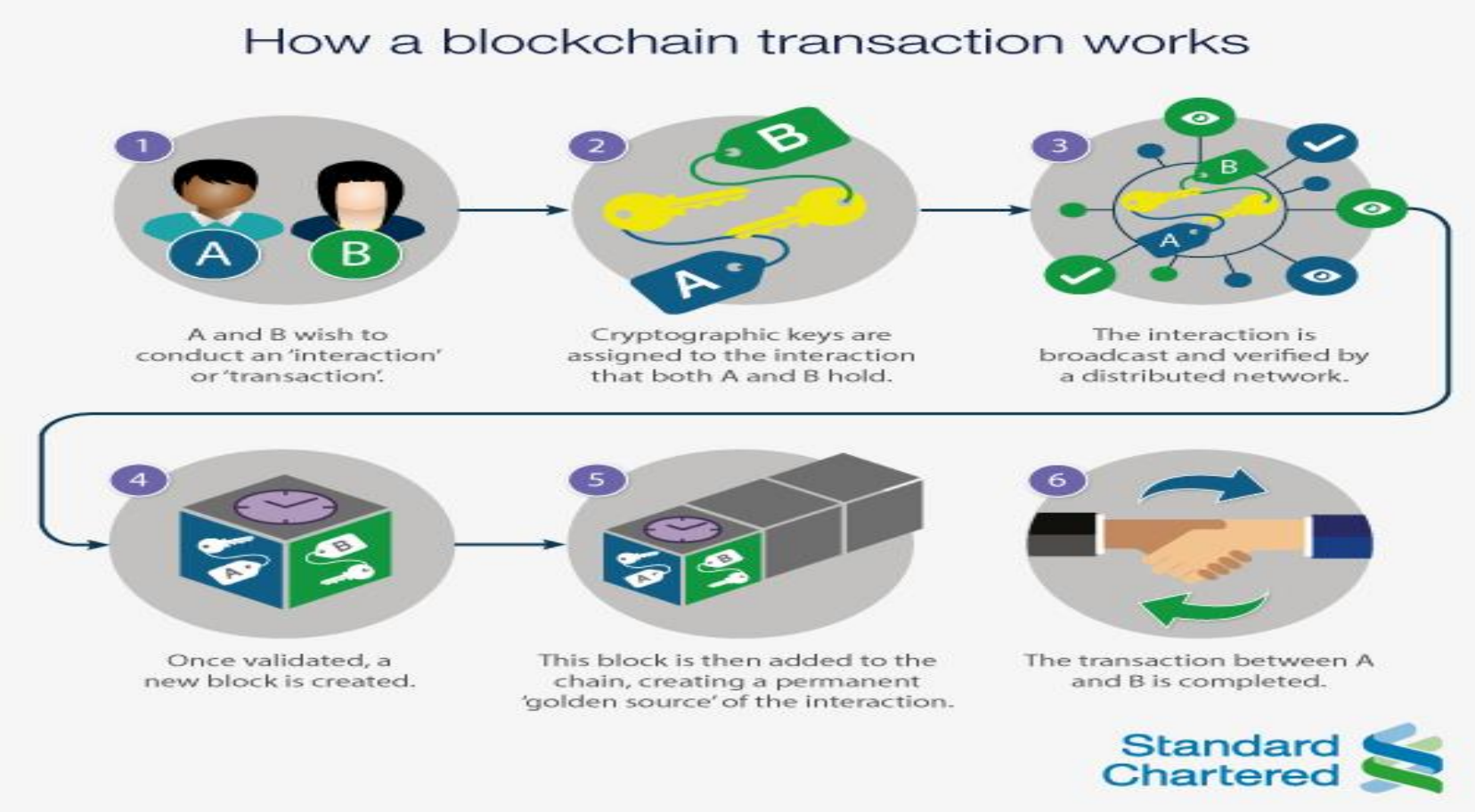
Bitkoin Blokçeynində blok strukturu



Bitkoin blokçeyninin vacib xüsusiyyəti

- Hər blokun HƏŞi öncəki blokun HƏŞ-i istifadə edilməklə formalaşır. Bu o deməkdir ki, keçmişə aid məlumatları dəyişmək mümkün deyil;

Blokçeyn necə işləyir



Ethereum (Efirium)

2015 – ci ildə təqdim edilib. İlk İCO layihəsi olmuşdur və qısa müddətdə 18 milyon toplaya bilmişdir.

Yaradıcısı: Vitalik Buterin (Rusiya və Kanada vətəndaşı), 31.01.1994

https://www.myetherwallet.com/#generate-wallet

Ethereum (Efirium)

- Vitalik Buterini maliyyələşdirən Piter Til (PayPal sahibi) olmuşdur;
- Bitkoindən fərqli olaraq Efirium ödəniş vasitəsi kimi geniş istifadə edilmir. Bu günə yalnız bir neçə internet-mağaza efiriumla ödənişləri qəbul edir (amazon (dolayı), overstock, ...);
- Prof of stake təhlükəsizlik protokolundan istifadə edir. Bu o deməkdir ki, blokları bağlamaq hüququ daha çox Efirə malik olanlardadır;
- Maner bir blok üçün 5 Efir qazanır;
- Bitkoindən fərqli olaraq Efirin emissiyasına məhdudiyyət yoxdur;

Ripple (XPR)

- Ripple ən geniş yayılmış və etibarlı kriptovalyutadır;
- Ripple banklar və digər maliyyə institutları arası ödənişlər şəbəkəsidir;
- Bu şəbəkə vasitəsi ilə həm adi Fiat pullar, kriprovalyutalar və digər aktivlər (o cümlədən qızıl) ötürülə bilər;
- Banklararası digər ödəniş şəbəkələri ilə müqaisədə Ripple-nin üstünlükləri:

- Yüksək sürət (ödənişlər cəmi 5-10 saniə çəkir);
- Təhlükəsizlik;
- Konfidensallıq;
- Xidmətin ucuzluğu.
- Ripple proqram təminatı Bitkoinin Farkı deyil;

Ripple

- Bu kriptovalyuta ovlanmır. Onu yalnız almaq və ya öz hesablayıcı resurslarınızı Ripple əməkdaşlıq etdiyi elmi və səhiyyə layihələrə təqdim etməklə əldə etmək mümkündür;
- Ripple yarandığı zaman cəmi yüz milliard Ripple sikkəsi buraxılıb istifadəyə. Bu artırıla bilməz. Hələ ki dövriyyədə təxminən 38 milliard Ripple sikkəsi var;
- Banklar arası ödənişlər edildikdə sistem ən uğurlu mübadilə variantla bunu edir;
- Banklar sistemə qoşulmağa təşviq edilir. Qoşulduqda onlara milyonlarla Ripple sikkəsi hədiyə edilir;
- https://ripple.com/

ICO (Initial Coin Offering)

Təxmini analoq – İPO (Initial Public Offering)

İCO hazırda, əsasən yeni kriptovalyutaların, kriptovalyuta birjalarının, müxtəlif blokçeyn alətlərinin yaradılması məqsədini daşıyan yeni startapların sərmayə (investisiya) toplamaq üsuludur. Fərq əsasən ondadır ki, İCO zamanı mülkiyyətdə yox gələcək məhsulda paylar satılır. Bu payların vahidinə TOKEN deyilir.

İCO-nu KROWDFUNDING (ing. Xalq Maliyyələşdirməsi. Termin 2006-cı ildən işlədilsədə üsulun tarixi böyükdür) növü kimi qeyd edirlər.

Ekspertlərin rəyincə, İCO vasitəsi ilə əldə edilən 1 USD vençur fondları vasitəsi ilə əldə olunan 3 USD-yə ekvivalentdir.

İCO xüsusi meydançalarda (birjalarda) elan edilir və elə buradaca TOKENlər satılır.

https://icotracker.net/

2016-cı ildə İCO bazarında 300 mln.USD tıoplanmışdır. Bu il artıq miliardı keçib.

TOKEN

Təxmini analoq – səhm.

Token bəzi birjalarda alınır və satılır. Məsələn: Poloniex

https://poloniex.com/

Tokenlər adi valyutaya və ya kriptovalyutaya alınır və satılır.

Bitkoini də ilk token hesab etmək olar. Maynerlər maraqlandırmaq üçün onlara məhz bitkoin ödənilir.

Məsələn, Siz hansısa yeni sosial şəbəkəni yaradırsınız, Sizə maliyyə gərəkir, Siz İCO elan edirsiniz, bu zaman sizin tokenlər yeni yaradılan sosial şəbəkədə reklam dəqiqələri ola bilər.

İCO prosesi

1. İdeyanızı anlaşılan dildə təsvir edirsiniz

2. İdeyanızın gerçəkləşməsi üçün tələb olunan maliyyə vəsaitini hesablayırsınız

3. TOKENlərin sayını müəyyənləşdirirsiniz

4. Layihənizi elan edirsiniz və reklam kompaniyasını aparırsınız (o cümlədən professional və sosial şəbəkələrdə)

5. TOKEN-lərin paylanması

6. Layihənin gerçəkləşdirilməsi

SMART kontraktlar

SMART akronimi ilk dəfə 1981-ci ildə bir məqalədə istifadə edilib və akronimdəki hərflər: *Specific, Measurable, Assignable (*Achievable*), Realistic (*Relevant), *Time-related (*Time-bound*)*

SMART kontrakt termini Vitalik Buterin tərəfindən təklif edilib. Məqsəd, SMART kontraktlara keçməklə öhdəlikləri blokçeyn vasitəsi ilə axıra çatdırmaq. Yəni yenə də banklarsız.

Zəif tərəfləri: 1) mürəkkəblik (xüsusi dilə çevrilməlidir); 2) dəyişgənlik; 3) qanunvericiliyin hazır olmaması...

Hələ ki, müxtəlif mərqoşmaların tədbiqi mümkün görünür.

TƏŞƏKKÜRLƏR

bagirov.sabit@gmail.com