RƏQƏMSAL İQTİSADİYYAT, BLOKÇEYN, KRİPTOVALYUTA

Sabit Bağırov

17 Noyabr, 2017

Təqdimatın içindəkiləri:

- Rəqəmsal iqtisadiyyat,
- BLOKÇEYN,
- KRİPTOVALYUTA,
- BİTKOİN,
- Efirium,
- Mayninq,
- Smartkontrakt,
- İCO,
- TOKEN

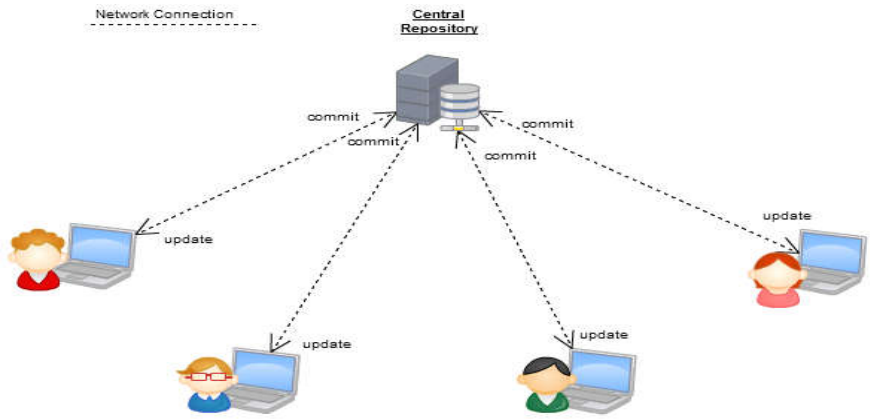
Rəqəmsal iqtisadiyyat

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.

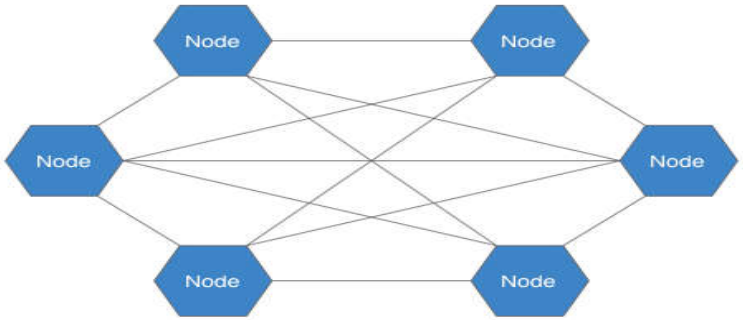
Böyük Britaniyanın İnternet iqtisadiyyatı 2012-ci ildə ÜDM-in 8.3%, 2-16-cı ildə isə 12%-nə bərabər olmuşdur.

Mərkəzli və mərkəzsiz sistemlər.



Üstünlük: İnzibatçılığın, təkmilləşdirmənin, miqyasın artırılması sadəliyi

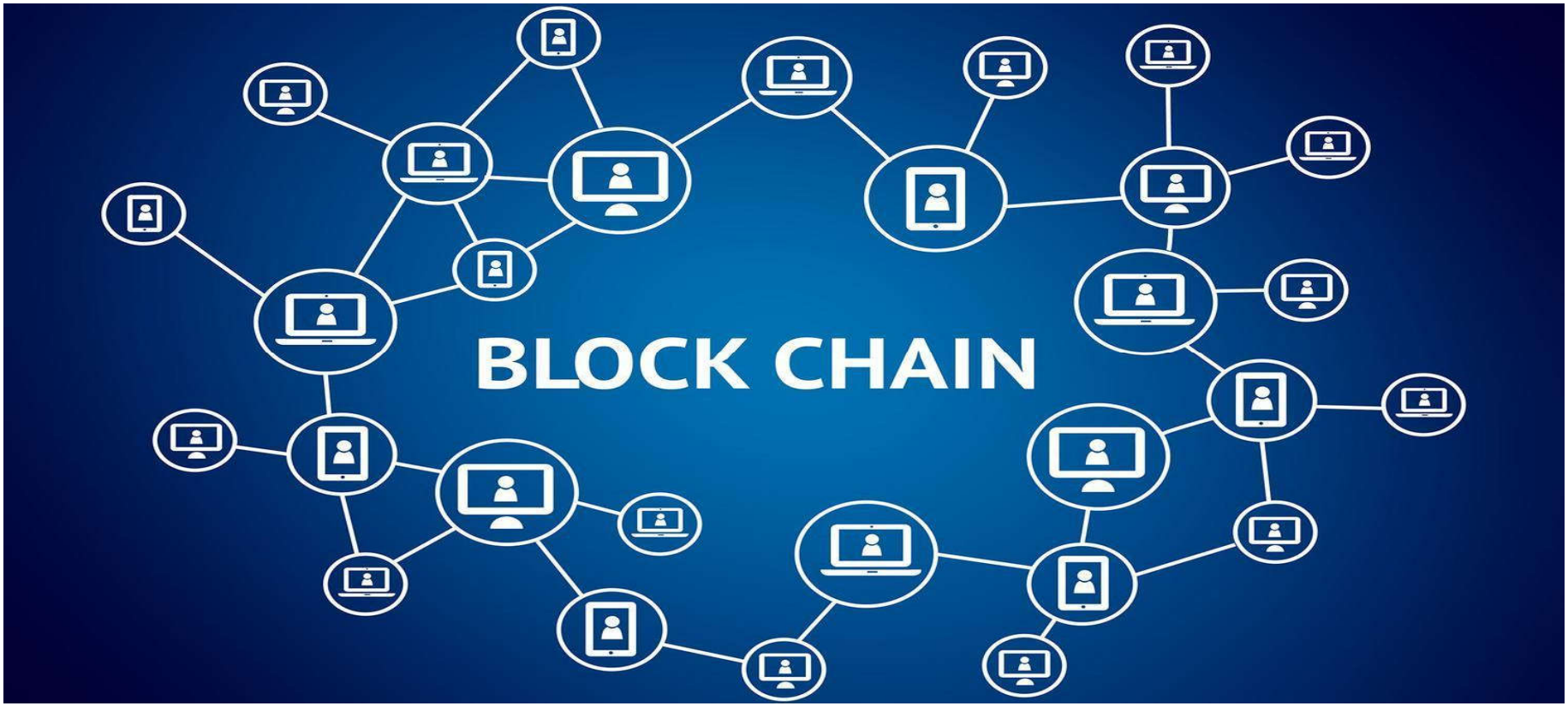
Zəif cəhədi: Kənar müdaxilə təhlükəsi



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 paylaşılması**. 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.

Blokçeynin tədbiqi

1. Müxtəlif sahələrdə istifadənin mümkünlüyü söylənilir (torpaq kadastrı, 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;
5. Tədbiqi gecikdirən əsas amillər:
   - Qanunvericiliklə hələ ki tənzimlənməməsi;
   - Hökumətlərin şübhə ilə yanaşması;
   - Bank sektorunun ciddi ehtiyatlanması və s.

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, ……
- EXCHANGE: https://changelly.com/exchange/BTC/ETH/1?ref_id=coinmarketcap

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, 10 noyabr – Bitkoinin dövriyyəsi = 119 mlrd, 1 Bitkoin =

Bitkoin

- Virtual pul vahididir;
- Yaradıcısı Satoşi Nakamoto sayılır (şəxsin və ya qrupun adı);
- Replikasiya (verilərin sinxronlaşdırılması) problemini həll edir;
- İnamsızlıq problemini həll edir;
- “proof of work” (işin sübutu) prinsipinə əsaslanır;
- Hesablanmır – «ovlanır» - hasil edilir. Bu prosesə MAYNİNQ deyilir;
- «Ovlayanlar» - «mədənçilərdir» (mayninqçilər) adlanır;
- «Ovlama» xüsusi proqram sistemi vasitəsi ilə həyata keçirilir;
- Proqram sistemi pulsuz əldə edilə bilər: https://www.nicehash.com/

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;
- Hər 10 dəqiqədən bir bütün toplanmış tranzaksiyalar cüt-cüt Haşlanır və yoxlanılır;
- Uğurlu yoxlamanın sonunda yeni blok öncəki bloklara əlavə edilir;

Ethereum

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

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

- 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 onlar milyonlarla Ripple sikkəsi hədiyə edilir;
- https://ripple.com/

Haş funksiyalar

$$y = f(x)$$

Burada x – müəyyən işarələr ardıcıllığıdır; y – funksiyaya uyğun alınan şifrdir;

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

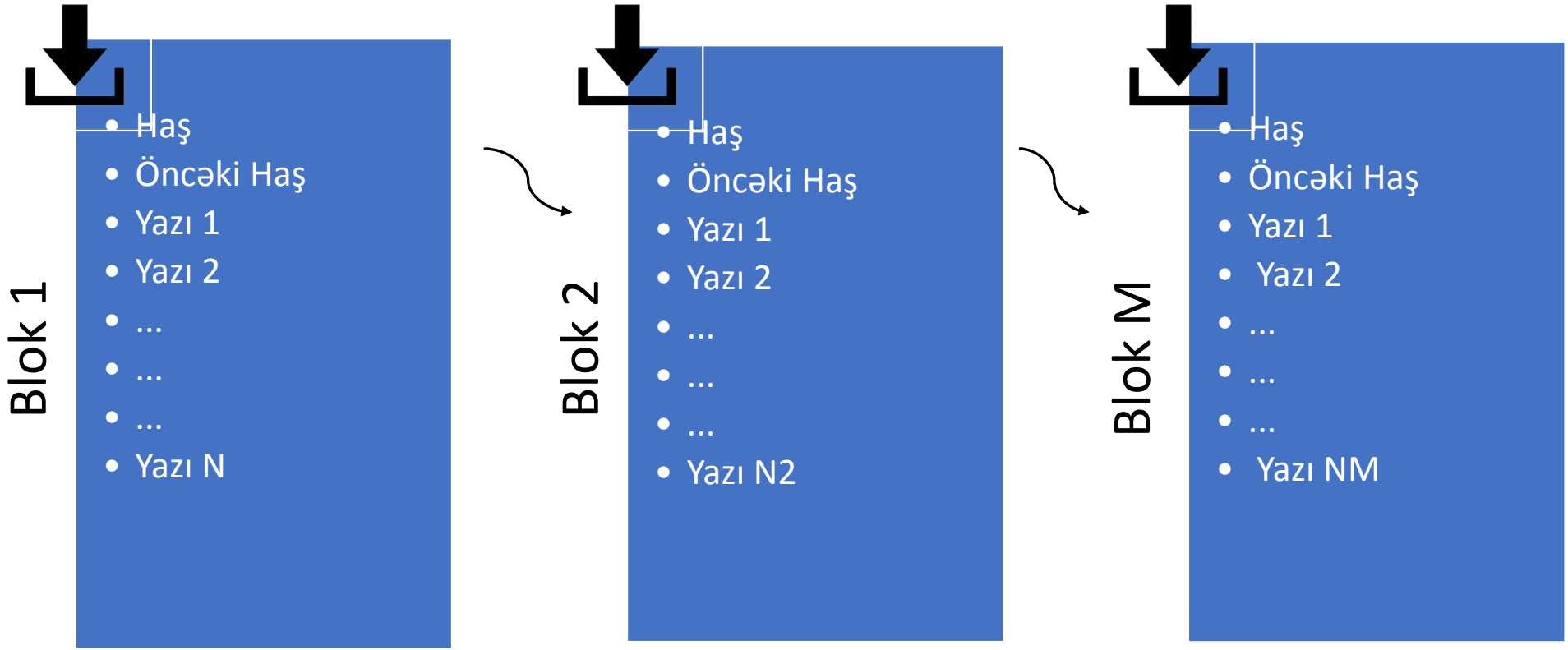
$$y = \sum_{i=1}^{n} x(i)$$

2. İstifadə edilən Haş funksiyalar: DM-5, DM-6E, Sha – 256, ...

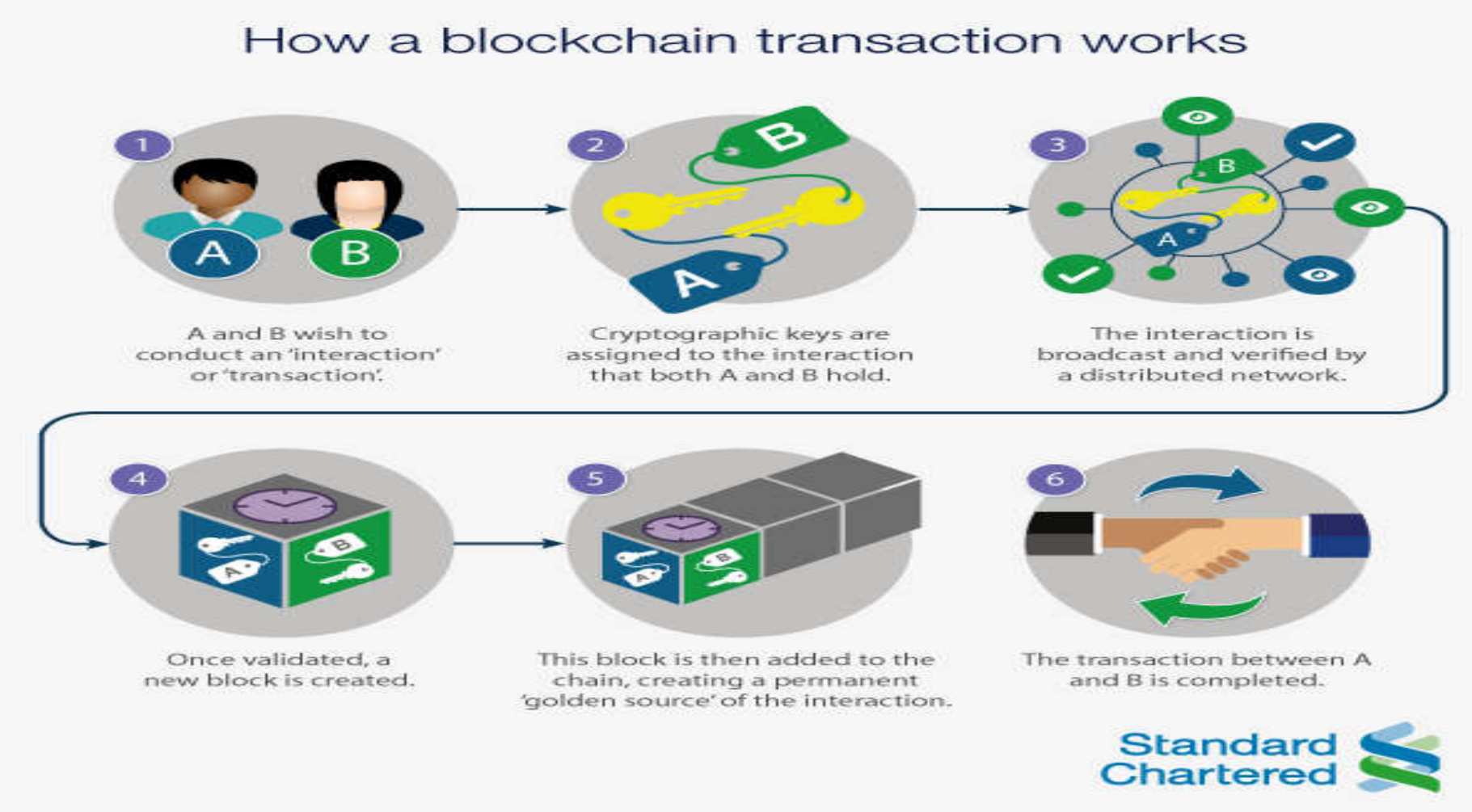
3. Digər növ funksiyalar

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

Bloklar


Blok 1
Haş
Öncəki Haş
Yazı 1
Yazı 2
...
...
...
Yazı N
Blok 2
Haş
Öncəki Haş
Yazı 1
Yazı 2
...
...
...
Yazı N2
Blok M
Haş
Öncəki Haş
Yazı 1
Yazı 2
...
...
...
Yazı NM

Blokçeyn necə işləyir



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 kontraktlar keçməklə öhdəlikləri ...

İnternetin həyatımıza töhvələri:

1-ci mərhələ - Məlumatların uçotu

- Elektron ünvan və yazışma;
- Elektron ticarət;
- Sosial Şəbəkələr;
- Mobil əlavələr;
- Böyük məlumat bazaları;
- Bulud hesablamaları;
- Xakerlər, Spaymerlər, Kibermoşenniklər

2-ci mərhələ - Dəyərlərin və Əşyaların interneti

TƏŞƏKKÜRLƏR