Kriptovalūtas:

Kas ir kriptovalūtas, kāpēc un kā tas tika rādītās.

Kādā ir kriptovalūtu nākotne.

Vai es varu pats radīt kriptovalūtu?

Justīna HUDENKO, *Dr.oec*
IEVF docente

202.gada 09.aprīlī

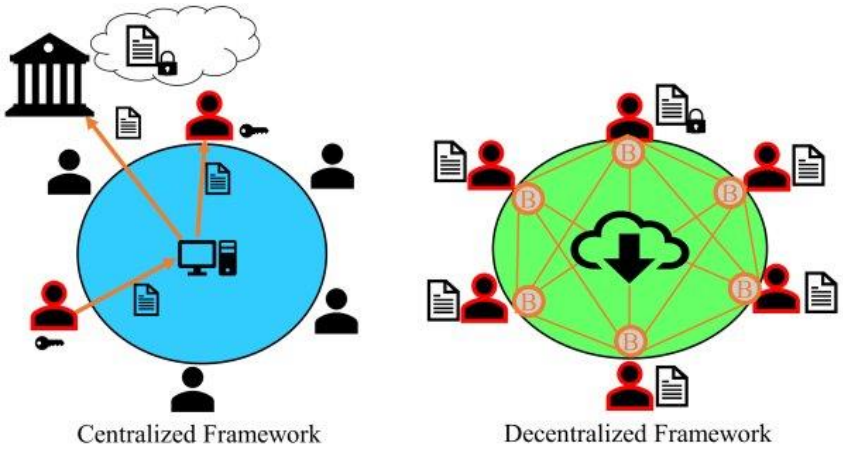
RTU Bērnu un jauniešu universitāte

Kas ir kriptovalūtas, kāpēc un kā tas tika rādītās.

Kas ir kriptovalūta

- Kriptovalūta ir aktīva digitālā forma.
- Visas tradicionālās tiešsaistes maksājumu platformas pieder dažām organizācijām.
- Kriptovalūtu gadījumā jūs varat izmantot bezmaksas programmatūru, lai nosūtītu līdzekļus citiem lietotājiem, bez starpniekiem.

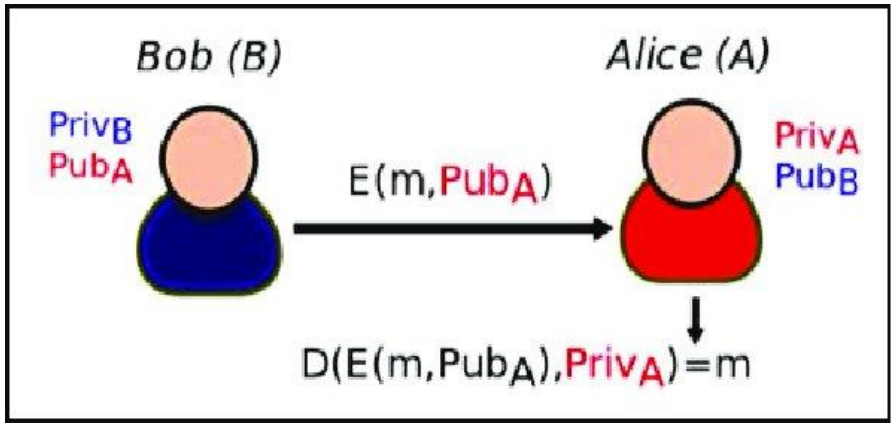
Kā tas strādā?



- Līdzekļi netiek nosūtīti!
- Tiek nosūtīta informācija par darījumu atklātā reģistrā kuru visi var redzēt;
- Visiem tīkla dalībniekiem ir datu bāzes kopijas, kas tiek glabātas savās ierīcēs, un viņi pastāvīgi sazinās viens ar otru, lai sinhronizētu jaunu informāciju.
- Kad lietotājs veic maksājumu, viņš to tieši pārraida vienādranga tīklā, kuram nav centralizētas bankas vai naudas pārvedumu apstrādes iestādes.

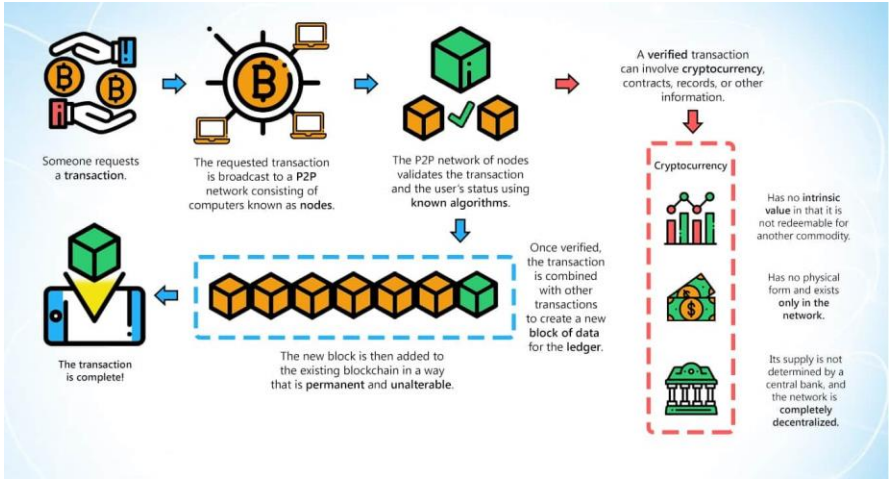
Kāpēc «kripto»

- Izmanto publiskās atslēgas kriptogrāfiju (PKC), jeb asimetrisku kriptogrāfiju: izmanto gan privāto, gan publisko atslēgu
- PKC shēmā publisko atslēgu informācijas šifrēšanai izmanto sūtītājs (to koplieto), savukārt privāto atslēgu izmanto saņēmējs, lai to atšifrētu - var lasīt tikai persona, kurai ir atbilstošā privātā atslēga.
- Asimetriskas šifrēšanas algoritmu iegūst, reizinot divus skaitļus (bieži vien divus lielus pirmskaitļus). Šifrēšana un atšifrēšana ir saistīta ar sarežģītām matemātiskām darbībām.



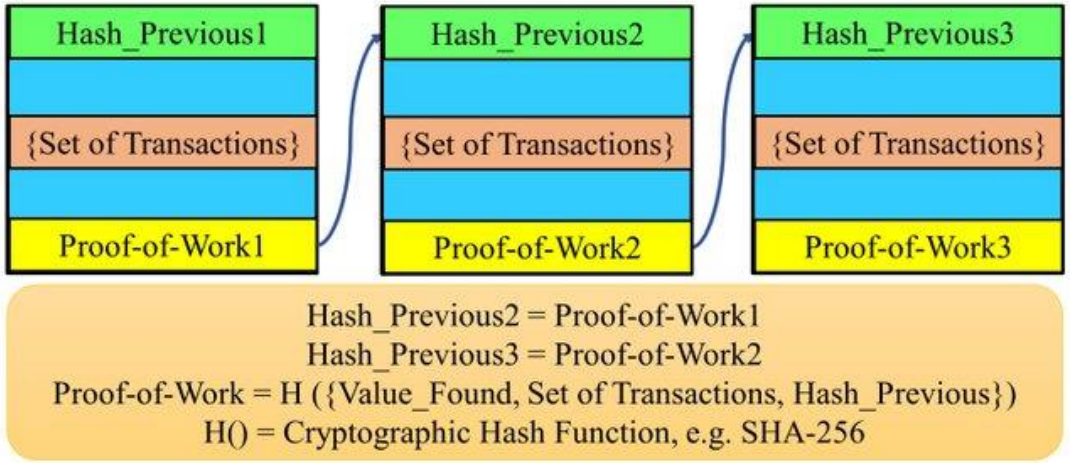
Blokķēde

- Blokķēde ir sava veida datubāze: šūnu kopums izklājlapā.
- Blokķēdes datus nevar mainīt - var pievienot tikai jaunu informāciju.
- Katrs ieraksts (saukts par bloku) datubāzē ir kriptogrāfiski saistīts ar iepriekšējo ierakstu - katram jaunajam ierakstam ir jābūt sava veida pēdējā ieraksta jaucējumam.
- Blokķēde ir nemainīga: ja bloks mainās, mainās arī pirkstu nospiedums. Un tā kā šī pēda ir iekļauta nākamajā blokā, mainās arī nākamais bloks.
- Ikviens var lejupielādēt blokķēdi un palaist pilnu tās kopiju savā datorā.



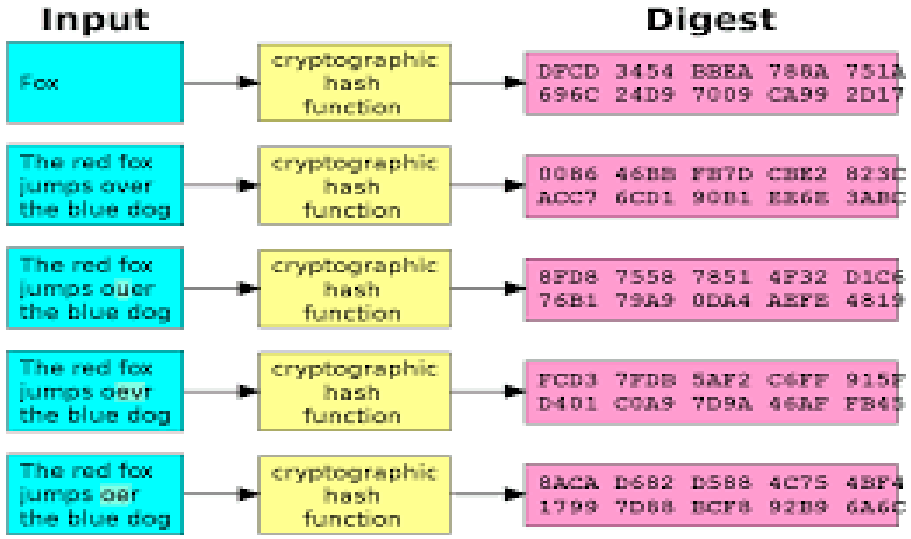
Vienprātības algoritms

- Vienprātības algoritms ir mehānisms, ar kura palīdzību lietotāji un programmas var koordinēt savas darbības izplatītajā tīklā.
- *Proof of Work* ir sistēma koordinētu tīkla lietotājus:
  - prasība lietotājiem, kuri vēlas pievienot blokus, pretī nodrošināt sava godīga darba garantiju (skaitļošanas jaudu, kriptovalūtu vai reputāciju);
  - par šo darbu ir īpaša atlīdzības sistēma;
  - caurspīdīgums.



Hash

- Darba apliecinājums (PoW) sajauc datus, ko vēlas pievienot, līdz tiek atrasts piemērots kriptogrāfiskās mīklas risinājums. Jaukšana (*hesh*) ir patvaļīga burtu un ciparu kopa, kas tiek izveidota, kad dati tiek apstrādāti, izmantojot jaucējfunkciju. Ja vēlreiz sajaucat tos pašus datus, jūs iegūsit to pašu rezultātu, bet, mainot vismaz vienu vērtību, jaukšana kļūs pavisam cita.
- Lielajās blokķēdēs ir ārkārtīgi grūti atrast piemērotu jaucējfunkciju.

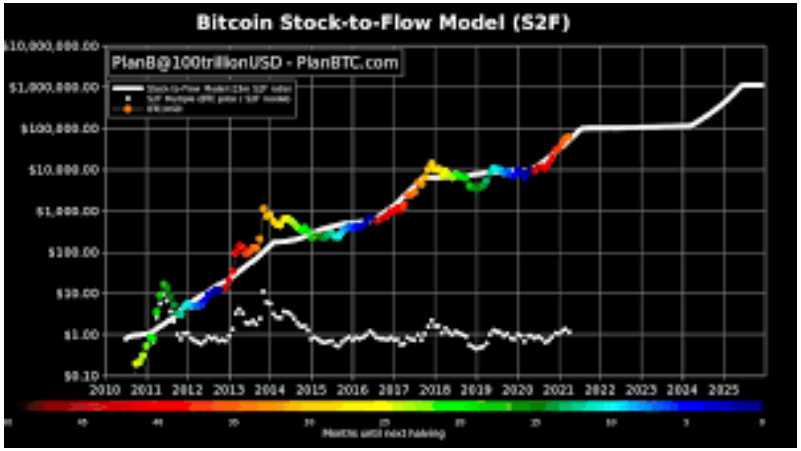


Kāpēc?

- Brīva no ierobežojumiem: centralizētie maksājumu pakalpojumi var iesaldēt kontus vai novērst darījumus.
- Tīkla dizains padara to izturīgu pret hakeru un citu iebrucēju uzbrukumiem.
- Lēts un ātrs maksāšanas veids: Cilvēks otrā pasaules malā var saņemt naudu no jums dažu sekunžu laikā. Maksa par darījumu ir ievērojami mazāka nekā starptautiskā naudas pārskaitījuma maksa.

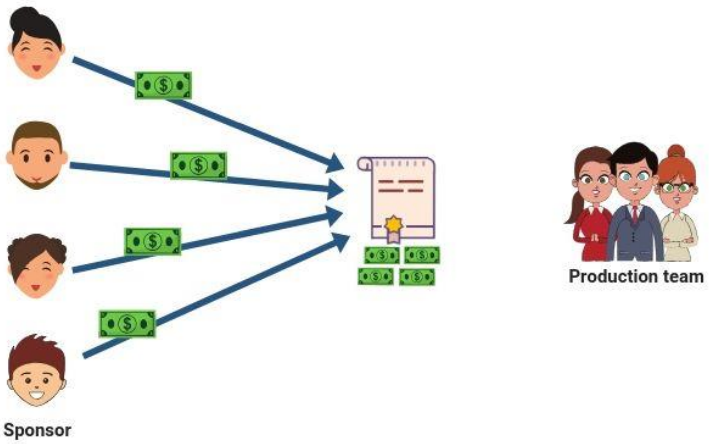
Kriptovalūta ≠ *Bitcoin*

- *Bitcoinam* ir *permissionless*, t.i. monētas var nosūtīt un saņemt ikviens, kam ir interneta pieslēgums.
- *Bitcoin* ir ieguvis iesauku "digitālais zelts" ierobežotā pieejamo monētu (21 milj) skaita dēļ. Vēl ne visas vienības ir apgrozībā iegūti 90%.
- Vienīgais veids, kā izveidot jaunas monētas, ir process, ko sauc par ieguvi – blokķēdes bloku pievienošana - atrisinot konkrētu kriptogrāfisku mīklu.
- Bitcoin ir pilnīgi likumīgs lielākajā daļā pasaules valstu.
- Bitcoin viedā līguma valoda ir ārkārtīgi ierobežota un slikti piemērota lietojumprogrammām, kas nav saistītas ar darījumiem.



Ethereum

- Ethereum iespējas ir plašākas par maksāšanu – var izmantot savu kodu un mijiedarboties ar citu lietotāju izveidotajām aplikācijām caur «viedājiem līgumiem»
- Ethereum ir protokols, bet valūtu, ar kuru tas darbojas, sauc par ēteri (vai ETH).
- Jebkurš lietotājs jebkurā vietā pasaulē var palaist lietojumprogrammu.
- Lai nošifrētu izmanto procesu, ko sauc par jaukšanu: datu daļa veido unikālo identifikatoru (jaucējs).



Kādā ir kriptovalūtu nākotne.

Trending

See more >

#	Name	Price	24h
1	STEPN	$2.14	▲2.51%
2	Animal Concerts	$0.02432	▲2.74%
3	Minifootball	$0.0...01086	▲26.05%
4	TABOO TOKEN	$0.003017	▼0.04%
5	PancakeSwap	$8.71	▼1.89%
6	Adadao	$0.05412	▼1.16%
7	NEAR Protocol	$17.89	▲14.66%
8	SXP	$1.33	▼2.86%
9	Solana	$113.95	▼3.21%
10	Shiba Inu	$0.00002428	▼2.06%

Biggest Gainers

See more >

#	Name	Price	24h
1	Sakura Bloom	$0.00009753	▲490.28%
2	Web3 ALL BEST ICO	$0.001098	▲197.55%
3	Ratscoin	$0.000000007007	▲151.10%
4	NFT All Best ICO	$0.0001373	▲147.54%
5	Metaverse ALL BEST ICO	$0.0003243	▲138.95%
6	Gera Coin	$1.07	▲122.90%
7	AME Chain	$0.01408	▲86.33%
8	CAPITAL X CELL	$0.003105	▲75.11%

Biggest Losers

See more >

#	Name	Price	24h
1	HelpSeed	$0.00000004037	▼99.91%
2	WonderHero	$0.003048	▼99.13%
3	Crypto Shield	$0.000001493	▼97.35%
4	Dark Matter	$0.00001603	▼61.09%
5	Beast Masters	$0.0001407	▼55.73%
6	Ruff	$0.001537	▼50.15%
7	Art Rino	$0.04687	▼48.76%
8	Savanna	$1.81	▼46.39%
9	Shisha	$0.000006689	▼46.16%
10	Ubex	$0.0001628	▼45.83%

Kriptotirdzniecība

- Kriptovalūtas spekulācijas (peļņas gūšana īstermiņā) mūsdienās ir viens no visizplatītākajiem lietošanas gadījumiem.
- Kriptovalūtu tirgu izprot veicot tehnisko analīzi: cenu vēsturi, diagrammas un cita veida tirgus datus, lai atrastu darījumus ar labu iespēju gūt peļņu.

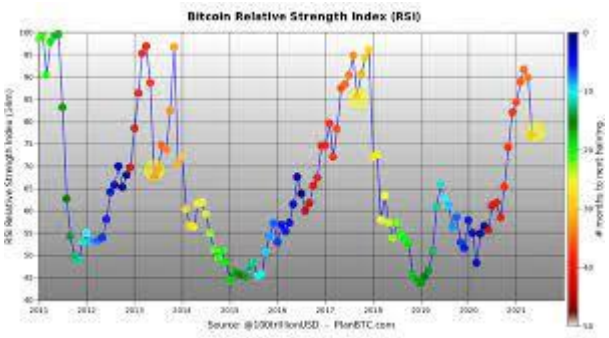
Šeit varat pamēģināt savus spēkus testa režīmā:

https://testnet.binancefuture.com/en/futures/BTCUSDT

Pamācība:

https://www.youtube.com/watch?v=C43JTuu0is0

Galvenie indikatori



- *Relative Strength Index* (RSI) ir rādītājs, uz kura pamata var secināt, vai aktīvs ir pārpirkts vai pārpārdots:
  - ja cenai augot rādītājs palielinās, augšupejoša tendence ir spēcīga un pircēju nāk arvien vairāk.
  - ja rādītāja mērs samazinās un cena pieaug, tas var norādīt, ka pārdevēji drīzumā var iegūt kontroli pār šo tirgu.

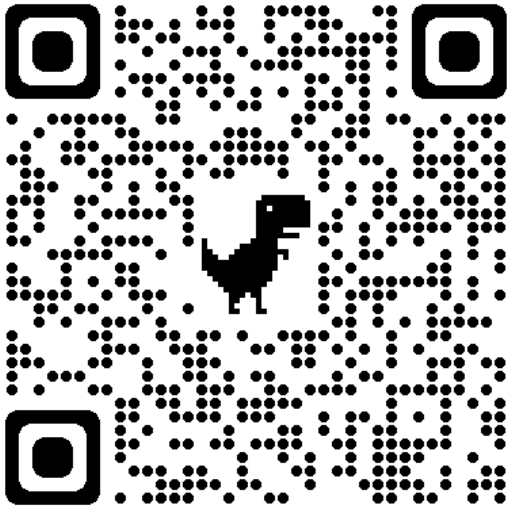
  Tradicionālā RSI interpretācija ir diagrammas līnijas digitālajos rādītājos: ja tas ir virs 70, tad aktīvs tiek pārpirkts, un, ja tas ir mazāks par 30, tad aktīvs tiek uzskatīts par pārpārdotu.
- *Moving average* (MA) izlīdzina cenu svārstības, filtrējot tirgus troksni un izceļot tendences virzienu.
- *Moving Average Convergence Divergence* (MACD) norāda uz aktīva nākotnes cenas kustību (var iegūt priekšstatu par pašreizējās tendences stiprumu), izmantojot divu mainīgo vidējo vērtību attiecības. Tas sastāv no divām līnijām:
  - MACD līnija tiek aprēķināta, atņemot 26 dienu MA no 12 dienu MA
  - signāla līnija, kas ir 9 dienu EMA
- Bolindžer band (BB) mēra tirgus nepastāvību un nosaka, vai aktīvs ir pārpirkts vai pārpārdots. Indikators sastāv no trim līnijām:
  - MA (vidējā josla),
  - augšējās un apakšējās joslas - ir divas standarta novirzes no mainīgā vidējā.

Kriptoinvestīcijas

Kriptoinvestīciju mērķis ir maksimāli palielināt sagaidāmo atdevi un samazināt iespējamo risku: ieguldījumu horizonta noteikšana, riska apetīte u.c. Vairāku viena no otras neatkarīgu aktīvu klašu apvienošana ir efektīvs veids, kā izveidot līdzsvarotu portfeli:

- Aktīvu sadale - kapitāls ir jāsadala starp ieguldījumu portfeļa aktīvu **klasēm**.
- Diversifikācija - kapitāla sadale šajās aktīvu klasēs.

Šeit varat pamēģināt savus spēkus spēļu režīmā:



Vai es varu pats radīt kriptovalūtu?

Kā izveidot krptovalūtu

- Lejupielādejiet bāzes kodu: github.com, https://dev.cryptolife.net
- Pārliecināties, vai datorā ir visas nepieciešamās bibliotēkas pareizam darbam ar kodu;
- Izvēlaties savas kriptovalūtas nosaukumu un izmainiet noklusējuma nosaukumu *FooCoin* uz jūsu izvēlēto. Ņemiet vērā, ka būs jāmaina vairākos reģistros: FooCoin – XxxCoin; FOOĊOIN – XXXCOIN; FOO – XXX; Foo – xxx;
- Tā kā visas darbības tiek veiktas, izmantojot internetu, programmai ir jākonfigurē tīkla porti, caur kuriem tiks pārsūtīti visi dati;
- Nosakiet, cik XXXCoin pienākas par jauno bloku veidošanu un cik XXXcoinu var saražot diennakts laikā;
- Izveidojiet savas ikoniņas un vizuālo tēlu.

Vai arī pamēģināt klonēt esošās valūtas un pievienot tām savas idejas: https://youtu.be/dlEHxys8ynU

Paldies slaida vietā:

Galvenie kiberuzbrukumu veidi:

- pikšķerēšana (phishing),
- izspiedējvīrus (ransomware)
- ļaunatūra (malware)

Obligāti aizsargājiet savu datoru:

https://cert.lv/lv/