

# MATEMATINIAI MODELIAI APLINK MUS – KRIPTOVALIUTOS

R. Čiegis

Vilniaus Gedimino technikos universitetas  
e-mail: rc@vgtu.lt

Vasario 23 d., 2021, Vilnius

Viena iš efektyviausių šiuolaikinių metodikų, universaliai keičianti mūsų gyvenimo daugelį sričių yra matematinis modeliavimas.

- ▶ Pirma – tai yra naujų žinių gavimo būdas. Jis leidžia kurti naujas, efektyvesnes gamybos technologijas, išmaniuosius produktus, medžiagas, įrenginius, poveikio priemones – skaitmenines technologijas.

Viena iš efektyviausių šiuolaikinių metodikų, universaliai keičianti mūsų gyvenimo daugelį sričių yra matematinis modeliavimas.

- ▶ Pirma – tai yra naujų žinių gavimo būdas. Jis leidžia kurti naujas, efektyvesnes gamybos technologijas, išmaniuosius produktus, medžiagas, įrenginius, poveikio priemones – skaitmenines technologijas.
- ▶ Antra – šie pasiekimai leidžia pereiti prie virtualių produktų atsiradimo. Tai pakeičia įprastinius mus supančius objektus. Tačiau jie signalizuoja apie daug svarbesnius pokyčius.

Viena iš efektyviausių šiuolaikinių metodikų, universaliai keičianti mūsų gyvenimo daugelį sričių yra matematinis modeliavimas.

- ▶ Pirma – tai yra naujų žinių gavimo būdas. Jis leidžia kurti naujas, efektyvesnes gamybos technologijas, išmaniuosius produktus, medžiagas, įrenginius, poveikio priemones – skaitmenines technologijas.
- ▶ Antra – šie pasiekimai leidžia pereiti prie virtualių produktų atsiradimo. Tai pakeičia įprastinius mus supančius objektus. Tačiau jie signalizuoja apie daug svarbesnius pokyčius.
- ▶ Kol kas tai panašiau į mokslinę fantastiką – atsiranda Dirbtinio Intelektu supratimas. Tai reiškia, kad mes rengiamės susitikti su virtualiais mąstančiais objektais, kurie taps mūsų realybės dalimi. Tokia teleportacija galima ir netgi tikėtina.

## Klasikiniai matematinio modeliavimo etapai yra šie:

- ▶ Mus dominančio proceso, reiškinių ar veiklos apibūdinimas (statistiniai duomenys, atskirų dalių matematiniai modeliai, naudojame tai veiklai būdingą kalbą).

## Klasikiniai matematinio modeliavimo etapai yra šie:

- ▶ Mus dominančio proceso, reiškinių ar veiklos apibūdinimas (statistiniai duomenys, atskirų dalių matematiniai modeliai, naudojame tai veiklai būdingą kalbą).
- ▶ Modelio diskrečioji aproksimacija ir validavimas.

## Klasikiniai matematinio modeliavimo etapai yra šie:

- ▶ Mus dominančio proceso, reiškinių ar veiklos apibūdinimas (statistiniai duomenys, atskirų dalių matematiniai modeliai, naudojame tai veiklai būdingą kalbą).
- ▶ Modelio diskrečioji aproksimacija ir validavimas.
- ▶ Vis dažniau yra pasitelkiama galimybė sukurti tinkamą matematinį modelį apmokant Dirbtinį Neuroninį Tinklą

## Klasikiniai matematinio modeliavimo etapai yra šie:

- ▶ Mus dominančio proceso, reiškinių ar veiklos apibūdinimas (statistiniai duomenys, atskirų dalių matematiniai modeliai, naudojame tai veiklai būdingą kalbą).
- ▶ Modelio diskrečioji aproksimacija ir validavimas.
- ▶ Vis dažniau yra pasitelkiama galimybė sukurti tinkamą matematinį modelį apmokant Dirbtinį Neuroninį Tinklą
- ▶ Tiriamojo proceso, technologijos, veiklos optimizavimas – fizinius eksperimentus keičiame skaitiniu (virtualiuoju) modeliavimu.



- ▶ Tradicinis matematinio modeliavimo technologijos rezultatas: naujos ar tobulesnės išmaniosios, greitesnės, saugesnės, pigesnės ir t.t. technologijos, produktai, įrankiai, ginklai ar apsaugos priemonės, vaistai ar nuodai (priklausomai nuo to į kieno rankas patenka šie rezultatai).

- ▶ Tradicinis matematinio modeliavimo technologijos rezultatas: naujos ar tobulesnės išmaniosios, greitesnės, saugesnės, pigesnės ir t.t. technologijos, produktai, įrankiai, ginklai ar apsaugos priemonės, vaistai ar nuodai (priklausomai nuo to į kieno rankas patenka šie rezultatai).
- ▶ Šiame seminare kalbėsime apie kitą, netgi svarbesnę matematinio modeliavimo galimybę – sukuriamas ne fizinio proceso pakankamai tikslus virtualusis modelis, o **skaitmeninis (virtualus) produktas, kuris pakeičia realųjį fizinį objektą.**

- ▶ Tradicinis matematinio modeliavimo technologijos rezultatas: naujos ar tobulesnės išmaniosios, greitesnės, saugesnės, pigesnės ir t.t. technologijos, produktai, įrankiai, ginklai ar apsaugos priemonės, vaistai ar nuodai (priklausomai nuo to į kieno rankas patenka šie rezultatai).
- ▶ Šiame seminare kalbėsime apie kitą, netgi svarbesnę matematinio modeliavimo galimybę – sukuriamas ne fizinio proceso pakankamai tikslus virtualusis modelis, o **skaitmeninis (virtualus) produktas, kuris pakeičia realųjį fizinį objektą.**
- ▶ Tai ir kriptovaliutos – **bitkoinas.**



Aptarkime svarbiausias bet kurios valiutos (pinigų) funkcionavimo sąlygas ir reikalavimus:

- ▶ 1. Kas kontroliuoja visus pagrindinius valiutos funkcionavimo etapus? Tradicinės valiutos remiasi **centralizuoto valdymo modeliu**. Dažniausiai tai atlieka Valstybė ir Centrinis bankas.

Aptarkime svarbiausias bet kurios valiutos (pinigų) funkcionavimo sąlygas ir reikalavimus:

- ▶ 1. Kas kontroliuoja visus pagrindinius valiutos funkcionavimo etapus? Tradicinės valiutos remiasi **centralizuoto valdymo modeliu**. Dažniausiai tai atlieka Valstybė ir Centrinis bankas.
- ▶ 2. Nustatomas pinigų spausdinimo grafikas ir poreikis (tai atlieka Valstybė). Deja tada galimas pinigų spausdinimas valstybės skolų dengimui, sukeltis pinigų nuvertėjimą.

Aptarkime svarbiausias bet kurios valiutos (pinigų) funkcionavimo sąlygas ir reikalavimus:

- ▶ 1. Kas kontroliuoja visus pagrindinius valiutos funkcionavimo etapus? Tradicinės valiutos remiasi **centralizuoto valdymo modeliu**. Dažniausiai tai atlieka Valstybė ir Centrinis bankas.
- ▶ 2. Nustatomas pinigų spausdinimo grafikas ir poreikis (tai atlieka Valstybė). Deja tada galimas pinigų spausdinimas valstybės skolų dengimui, sukeliantis pinigų nuvertėjimą.
- ▶ 3. Pinigų (banknotų, monetų) apsauga nuo padirbinėjimo (Centrinis bankas, baudžiamoji atsakomybė už pinigų padirbinėjimą, teisinės priemonės).

Aptarkime svarbiausias bet kurios valiutos (pinigų) funkcionavimo sąlygas ir reikalavimus:

- ▶ 1. Kas kontroliuoja visus pagrindinius valiutos funkcionavimo etapus? Tradicinės valiutos remiasi **centralizuoto valdymo modeliu**. Dažniausiai tai atlieka Valstybė ir Centrinis bankas.
- ▶ 2. Nustatomas pinigų spausdinimo grafikas ir poreikis (tai atlieka Valstybė). Deja tada galimas pinigų spausdinimas valstybės skolų dengimui, sukeltis pinigų nuvertėjimą.
- ▶ 3. Pinigų (banknotų, monetų) apsauga nuo padirbinėjimo (Centrinis bankas, baudžiamoji atsakomybė už pinigų padirbinėjimą, teisinės priemonės).
- ▶ 4. Kliento mokumo patikrinimas (bankai tikrina klientų sąskaitų naudojimą, norėdami atidaryti sąskaitą banke turime pateikti asmeninius duomenis, informaciją apie darbinius santykius). Tačiau bankai užtikrina ir visos informacijos slaptumą, anonimiškumą,

Aptarkime svarbiausias bet kurios valiutos (pinigų) funkcionavimo sąlygas ir reikalavimus:

- ▶ 1. Kas kontroliuoja visus pagrindinius valiutos funkcionavimo etapus? Tradicinės valiutos remiasi **centralizuoto valdymo modeliu**. Dažniausiai tai atlieka Valstybė ir Centrinis bankas.
- ▶ 2. Nustatomas pinigų spausdinimo grafikas ir poreikis (tai atlieka Valstybė). Deja tada galimas pinigų spausdinimas valstybės skolų dengimui, sukeltis pinigų nuvertėjimą.
- ▶ 3. Pinigų (banknotų, monetų) apsauga nuo padirbinėjimo (Centrinis bankas, baudžiamoji atsakomybė už pinigų padirbinėjimą, teisinės priemonės).
- ▶ 4. Kliento mokumo patikrinimas (bankai tikrina klientų sąskaitų naudojimą, norėdami atidaryti sąskaitą banke turime pateikti asmeninius duomenis, informaciją apie darbinius santykius). Tačiau bankai užtikrina ir visos informacijos slaptumą, anonimiškumą,
- ▶ 5. Bankai yra atsakingi už **buhalterinės knygos** formavimą ir teisingumą, jie kontroliuoja, kad nebūtų vykdomos tokios veiklos, kaip "pinigų plovimas", svetimų sąskaitų panaudojimas.



Elektroniniai pinigai (internetinė prekyba, debetinės ir kreditinės kortelės) yra tik klasikinių pinigų funkcionavimo išmaniosios technologijos.

**Kriptovaliutos** irgi turi garantuoti **svarbiausius** suformuluotus reikalavimus. Tačiau tai pasiekama remiantis **DECENTRALIZUOTO** valdymo paradigma.

Decentralizuotas internetas, e-paštas – tai kiti siekiami tikslai.

Nei viename etape nelieka Centro (valstybės, centrinio banko, bankų buhalterinių knygų, su mūsų ID susietų sąskaitų).

Pinigų kiekis kinta pagal iš anksto patvirtintą algoritmą.

Didžioji dalis visuomenės pasitikime mūsų Valstybe, taigi norėdamos įsitvirtinti kriptovaliutos turi įrodyti savo pranašumus.

# Kripto valiutų funkcionavimas grindžiamas šiuolaikiniais MATEMATIKOS ir INFORMATIKOS rezultatais

# Kripto valiutų funkcionavimas grindžiamas šiuolaikiniais MATEMATIKOS ir INFORMATIKOS rezultatais

- ▶ 1. Kriptografijos algoritmais

## Kripto valiutų funkcionavimas grindžiamas šiuolaikiniais MATEMATIKOS ir INFORMATIKOS rezultatais

- ▶ 1. Kriptografijos algoritmais
- ▶ 2. Efektyviais decentralizuoto sprendimo priėmimo algoritmais

## Kripto valiutų funkcionavimas grindžiamas šiuolaikiniais MATEMATIKOS ir INFORMATIKOS rezultatais

- ▶ 1. Kriptografijos algoritmais
- ▶ 2. Efektyviais decentralizuoto sprendimo priėmimo algoritmais
- ▶ 3. Duomenų struktūromis ir jų realizavimo algoritmais

## Kripto valiutų funkcionavimas grindžiamas šiuolaikiniais MATEMATIKOS ir INFORMATIKOS rezultatais

- ▶ 1. Kriptografijos algoritmais
- ▶ 2. Efektyviais decentralizuoto sprendimo priėmimo algoritmais
- ▶ 3. Duomenų struktūromis ir jų realizavimo algoritmais
- ▶ 4. Našiųjų skaičiavimų technologijomis

## Kripto valiutų funkcionavimas grindžiamas šiuolaikiniais MATEMATIKOS ir INFORMATIKOS rezultatais

- ▶ 1. Kriptografijos algoritmais
- ▶ 2. Efektyviais decentralizuoto sprendimo priėmimo algoritmais
- ▶ 3. Duomenų struktūromis ir jų realizavimo algoritmais
- ▶ 4. Našiujų skaičiavimų technologijomis
- ▶ 5. Internetinėmis technologijomis



Nagrinėsime populiariausią kriptovaliutą – bitkoinus.

- ▶ Jie pradėti naudoti 2009 metais, per tą laiką gana smarkiai keitėsi visų veiklų skaitmenizavimas, virtualizavimas, atsirado naujos skaičiavimo ir internetinių technologijų kartos, naudojame 5G internetą.

Nagrinésime populiariausią kriptovaliutą – bitkoinus.

- ▶ Jie pradėti naudoti 2009 metais, per tą laiką gana smarkiai keitėsi visų veiklų skaitmenizavimas, virtualizavimas, atsirado naujos skaičiavimo ir internetinių technologijų kartos, naudojame 5G internetą.
- ▶ Tai, kad bitkoinai sėkmingai konkuruoja su kitomis kriptovaliutomis, parodo, jog pasirinkimai, kurie buvo užfiksuoti pagrindiniame protokole, **YRA** labai efektyvūs, inovatyvūs, įžvalgūs, atsparūs pokyčiams.

Nagrinėsime populiariausią kriptovaliutą – bitkoinus.

- ▶ Jie pradėti naudoti 2009 metais, per tą laiką gana smarkiai keitėsi visų veiklų skaitmenizavimas, virtualizavimas, atsirado naujos skaičiavimo ir internetinių technologijų kartos, naudojame 5G internetą.
- ▶ Tai, kad bitkoinai sėkmingai konkuruoja su kitomis kriptovaliutomis, parodo, jog pasirinkimai, kurie buvo užfiksuoti pagrindiniame protokole, **YRA** labai efektyvūs, inovatyvūs, įžvalgūs, atsparūs pokyčiams.
- ▶ Dabar galime įvertinti ir pasirinkto protokolo ribojimus, kuriuos sunku pakeisti, bet naudinga analizuoti.

## Nagrinėsime populiariausią kriptovaliutą – bitkoinus.

- ▶ Jie pradėti naudoti 2009 metais, per tą laiką gana smarkiai keitėsi visų veiklų skaitmenizavimas, virtualizavimas, atsirado naujos skaičiavimo ir internetinių technologijų kartos, naudojame 5G internetą.
- ▶ Tai, kad bitkoinai sėkmingai konkuruoja su kitomis kriptovaliutomis, parodo, jog pasirinkimai, kurie buvo užfiksuoti pagrindiniame protokole, **YRA** labai efektyvūs, inovatyvūs, įžvalgūs, atsparūs pokyčiams.
- ▶ Dabar galime įvertinti ir pasirinkto protokolo ribojimus, kuriuos sunku pakeisti, bet naudinga analizuoti.
- ▶ Žinomas principas, kad geriau mokytis iš svetimų klaidų. Bet ar taip darome?

- ▶ Nauji bitkoinai sukuriami apytiksliai kas 10 minučių. Šiandien jų vertė yra 6.25 BTC. Kas 4 metai šis skaičius yra mažinamas dvigubai (pradžioje tai buvo 50 BTC).  
Mažiausias bitkoino vienetas yra Satoshi:

$$1 \text{ BTC} = 1 \cdot 10^8 \text{ Satoshis.}$$

- ▶ Nauji bitkoinai sukuriami apytiksliai kas 10 minučių. Šiandien jų vertė yra 6.25 BTC. Kas 4 metai šis skaičius yra mažinamas dvigubai (pradžioje tai buvo 50 BTC).  
Mažiausias bitkoino vienetas yra Satoshi:

$$1 \text{ BTC} = 1 \cdot 10^8 \text{ Satoshis.}$$

- ▶ Toks geometrinės progresijos dėsnis garantuoja, kad galutinis pinigų kiekis yra ribojamas 21 mln., ir tai atsitiks 2140 metais. Taip pat visada yra žinomas egzistuojančių pinigų kiekis. Šiuo metu jau turime apie 18.6 mln. bitkoinų.

- ▶ Kokie yra BTC monetų nominalai: 1, 2, 5, 10, 20, 100, 500, 1000?

# BITKŪ MONETŲ SAVYBĖS

- ▶ Kokie yra BTC monetų nominalai: 1, 2, 5, 10, 20, 100, 500, 1000?
- ▶ Ne, monetos vertė gali būti bet kokia, ji užduodama 1 Satoshi tikslumu.



# BITKOINŲ MONETŲ SAVYBĖS

- ▶ Kokie yra BTC monetų nominalai: 1, 2, 5, 10, 20, 100, 500, 1000?
- ▶ Ne, monetos vertė gali būti bet kokia, ji užduodama 1 Satoshi tikslumu.
- ▶ Bitkoino monetos šeimininkas transakcijos metu **sumoka visą jos vertę** ir tada moneta išnyksta.

- ▶ Kokie yra BTC monetų nominalai: 1, 2, 5, 10, 20, 100, 500, 1000?
- ▶ Ne, monetos vertė gali būti bet kokia, ji užduodama 1 Satoshi tikslumu.
- ▶ Bitkoino monetos šeimininkas transakcijos metu **sumoka visą jos vertę** ir tada moneta išnyksta.
- ▶ Jeigu 10.337 BTC vertės moneta mokame už 2.12 BTC paslaugą, tai likusius 8.217 BTC pervedame į savo sąskaitą, sukurdami naują tokios vertės monetą.

# BITKOINŲ MONETŲ SAVYBĖS

- ▶ Kokie yra BTC monetų nominalai: 1, 2, 5, 10, 20, 100, 500, 1000?
- ▶ Ne, monetos vertė gali būti bet kokia, ji užduodama 1 Satoshi tikslumu.
- ▶ Bitkoino monetos šeimininkas transakcijos metu **sumoka visą jos vertę** ir tada moneta išnyksta.
- ▶ Jeigu 10.337 BTC vertės moneta mokame už 2.12 BTC paslaugą, tai likusius 8.217 BTC pervedame į savo sąskaitą, sukurdami naują tokios vertės monetą.
- ▶ Monetos vertės likutis tampa mokesčiu (**transaction fee**) tam tinklo atstovui, kuris įtraukia bloką su šia transakcija į Buhalterinę knygą (distributed ledger).

# SKAITMENINIO PARAŠO SCHEMA

Monetos savininkas patvirtina transakcijos teisėtumą **skaitmeniniu parašu** (pirmasis ir labai svarbus kriptografijos elementas).

Skaitmeninis parašas generuojamas koku nors **patikimu** viešojo rakto pasikeitimo algoritmu (pvz. RSA, diskrečiojo logaritmo algoritmais).

- ▶ 1. Generuojame atsitiktinį slaptąjį (privatųjį) raktą **sk**, tada apskaičiuojame jį atitinkantį viešąjį raktą **pk**.

# SKAITMENINIO PARAŠO SCHEMA

Monetos savininkas patvirtina transakcijos teisėtumą **skaitmeniniu parašu** (pirmasis ir labai svarbus kriptografijos elementas).

Skaitmeninis parašas generuojamas koku nors **patikimu** viešojo rakto pasikeitimo algoritmu (pvz. RSA, diskrečiojo logaritmo algoritmais).

- ▶ 1. Generuojame atsitiktinį slaptąjį (privatųjį) raktą **sk**, tada apskaičiuojame jį atitinkantį viešąjį raktą **pk**.
- ▶ 2. Tik šeimininkas gali pasirašyti dokumentą  $M$ :

$$sig := sign(sk, M).$$

# SKAITMENINIO PARAŠO SCHEMA

Monetos savininkas patvirtina transakcijos teisėtumą **skaitmeniniu parašu** (pirmasis ir labai svarbus kriptografijos elementas).

Skaitmeninis parašas generuojamas koku nors **patikimu** viešiojo rakto pasikeitimo algoritmu (pvz. RSA, diskrečiojo logaritmo algoritmais).

- ▶ 1. Generuojame atsitiktinį slaptąjį (privatųjį) raktą **sk**, tada apskaičiuojame jį atitinkantį viešąjį raktą **pk**.
- ▶ 2. Tik šeimininkas gali pasirašyti dokumentą  $M$ :

$$sig := sign(sk, M).$$

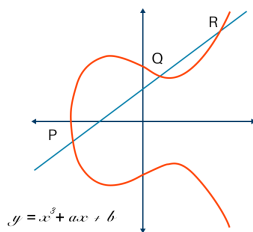
- ▶ 3. Visi gali patikrinti parašo teisingumą

$$M := verify(pk, sig).$$

# ELIPSINIŲ KREIVIŲ SKAITMENINIO PARAŠO ALGORITMAS

Bitkoinų protokole naudojamas kriptografinis ECDSA (Elliptic Curve Digital Signature Algorithm) algoritmas.

Jis remiasi elipsinių kreivių (pvz.  $y^2 = x^3 + ax + b$ ) taškų daugybos operacija.



$$P + Q + R = 0.$$

Egzistuoja greitieji daugybos algoritmai, bet nėra žinomi greitieji logoritmavimo algoritmai. Vėl tenka naudoti pilnąjį perrinkimą.

Viešojo rakto  $pk$  – public key pavyzdys:

044d05240cfbd8a2786eda9dadd520c1609b8593ff8641018d57703d02ba  
687cf2f187f0cee2221c3afb1b5ff7888caced2423916b61444666ca1216  
f26181398c

Formatas: taško  $P(x, y)$  koordinatės  $x$  ir  $y$ , jų ilgiai po 32 baitus

$$pk = 04 x y$$

Tada privataus rakto  $pk$  ilgis yra  $1 + 32 + 32 = 65$  baitai, arba 130 hex simbolių, arba 520 bitų.



Bitkoinų protokole viešajam raktui **pk** yra skirta dar viena svarbi ir įdomi savybė. Šis raktas yra naudojamas kaip kliento sąskaitos ID.

- ▶ Kiekvieną kartą, kai generuojamas viešasis raktas, **sukūriama nauja sąskaita**.

Bitkoinų protokole viešajam raktui **pk** yra skirta dar viena svarbi ir įdomi savybė. Šis raktas yra naudojamas kaip kliento sąskaitos ID.

- ▶ Kiekvieną kartą, kai generuojamas viešasis raktas, **sukūriama nauja sąskaita**.
- ▶ Kiekvienas žmogus tai gali padaryti pats, **nereikia jokių leidimų ar patikrinimų**.

Bitkoinų protokole viešajam raktui **pk** yra skirta dar viena svarbi ir įdomi savybė. Šis raktas yra naudojamas kaip kliento sąskaitos ID.

- ▶ Kiekvieną kartą, kai generuojamas viešasis raktas, **sukūriama nauja sąskaita**.
- ▶ Kiekvienas žmogus tai gali padaryti pats, **nereikia jokių leidimų ar patikrinimų**.
- ▶ Turimų sąskaitų skaičius yra neribojamas.

Bitkoinų protokole viešajam raktui **pk** yra skirta dar viena svarbi ir įdomi savybė. Šis raktas yra naudojamas kaip kliento sąskaitos ID.

- ▶ Kiekvieną kartą, kai generuojamas viešasis raktas, **sukūriama nauja sąskaita**.
- ▶ Kiekvienas žmogus tai gali padaryti pats, **neriekia jokių leidimų ar patikrinimų**.
- ▶ Turimų sąskaitų skaičius yra neribojamas.
- ▶ Nėra **tiesioginės galimybės** identifikuoti, kam priklauso viena ar kita sąskaita.

Bitkoinų protokole viešajam raktui **pk** yra skirta dar viena svarbi ir įdomi savybė. Šis raktas yra naudojamas kaip kliento sąskaitos ID.

- ▶ Kiekvieną kartą, kai generuojamas viešasis raktas, **sukūriama nauja sąskaita**.
- ▶ Kiekvienas žmogus tai gali padaryti pats, **neriekia jokių leidimų ar patikrinimų**.
- ▶ Turimų sąskaitų skaičius yra neribojamas.
- ▶ Nėra **tiesioginės galimybės** identifikuoti, kam priklauso viena ar kita sąskaita.
- ▶ Tačiau, **pilno anonimškumo** bitkoino adresai nesuteikia. Kaip matysime, tai yra kompromisas tarp kliento sąskaitos saugumo, mokėjimų patikimumo ir decentralizacijos principo.

- ▶ Kriptografinė santraukos funkcija  $h(x)$  kintamo ilgio (baigtinio) žodžius (strings)  $x$  atvaizduoja į fiksuoto ilgio žodžius – **suspaudimo savybė**.

- ▶ Kriptografinė santraukos funkcija  $h(x)$  kintamo ilgio (baigtinio) žodžius (strings)  $x$  atvaizduoja į fiksuoto ilgio žodžius – **suspaudimo savybė**.
- ▶ Tai vienakryptės funkcijos – duotajam  $x$  lengva apskaičiuoti vaizdą  $y = h(x)$ , bet žinant  $y$  **sunku surasti**  $x$  – **slėpimo savybė**.

- ▶ Kriptografinė santraukos funkcija  $h(x)$  kintamo ilgio (baigtinio) žodžius (strings)  $x$  atvaizduoja į fiksuoto ilgio žodžius – **suspaudimo savybė**.
- ▶ Tai vienakryptės funkcijos – duotajam  $x$  lengva apskaičiuoti vaizdą  $y = h(x)$ , bet žinant  $y$  **sunku surasti**  $x$  – **slėpimo savybė**.
- ▶ Mus domina santraukos funkcijos, kurios yra atsparios kolizijoms – duotajam  $x_1$  sunku surasti  $x_2 \neq x_1$ , kad galiotų lygybė  $h(x_1) = h(x_2)$ .



- ▶ Kriptografinė santraukos funkcija  $h(x)$  kintamo ilgio (baigtinio) žodžius (strings)  $x$  atvaizduoja į fiksuoto ilgio žodžius – **suspaudimo savybė**.
- ▶ Tai vienakryptės funkcijos – duotajam  $x$  lengva apskaičiuoti vaizdą  $y = h(x)$ , bet žinant  $y$  **sunku surasti  $x$  – slėpimo savybė**.
- ▶ Mus domina santraukos funkcijos, kurios yra atsparios kolizijoms – duotajam  $x_1$  sunku surasti  $x_2 \neq x_1$ , kad galiotų lygybė  $h(x_1) = h(x_2)$ .
- ▶ Matematinis uždavinys, kai žinome žodį (stringą)  $x$ , turime leistinų santraukos reikšmių aibę  $D$ , o reikia surasti tokį papildomą žodį  $n$ , kad galiotų sąlyga

$$h(n||x) \in D,$$

yra išsprendžiamas tik pilnojo perrinkimo metodu. Čia  $n||x$  yra stringas, gaunamas apjungus  $n$  ir  $x$ . Pavyzdžiui, aibei  $D$  priklauso santraukos, kurios prasideda  $m$  nuliių.

Santraukos funkcijos yra labai populiarus įrankis

a) realizuojant duomenų saugyklas debesijoje,

b) informacijos paieškos algoritmuose.

Bitkoinų protokole apibrėžta, kad viešojo rakto **pk** santrauką **pkh** skaičiuojame pritaikydami paeiliui dvi skirtingas hash funkcijas:

$$pkh = HASH160(pk) := RIPEMD160(SHA256(pk)).$$

SHA256 yra SHA-2 (Secure Hash Algorithm 2) algoritmų šeimos atstovas. Ši funkcija generuoja 256 bitų (32 baitų) santrauką. Suspaudimas atliekamas vykdant 64 iteracijas (rounds)

RIPEMD160 yra RIPEMD algoritmų šeimos atstovas. Ši funkcija generuoja 160 bitų (20 baitų) santrauką. Suspaudimas atliekamas vykdant 80 iteracijų (rounds)

Viešojo rakto **pk** santrauka **pkh** irgi apibrėžia tinklo dalyvio **adresą**.

pk

044d05240cfbd8a2786eda9dadd520c1609b8593ff8641018d57703d02ba  
687cf2f187f0cee2221c3afb1b5ff7888caced2423916b61444666ca1216  
f26181398c

SHA256(pk)

a8c0b9c1ee07b2442387c7f0f6ac32d646d7ff6d385e8762e989f634dda584a5

adresas HASH160(pk)

2e67490797078511cfde499434ed6a564ad41ef0

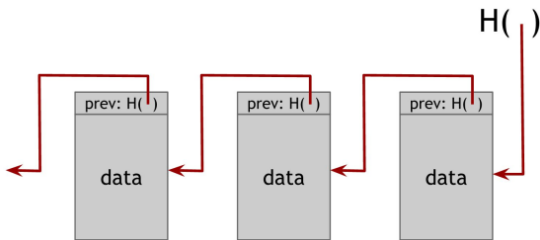
adresas BASE58(HASH160(pk))

eVkea3yfmMy7NYxHtMHoicLGuXm

# BLOKŲ GRANDINĖS

Bitkoinų saugumą garantuoja dvi pagrindinės technologijos. Tai **blokų grandinės** (blockchains) ir kriptografiniai transakcijų realizavimo algoritmai.

Blokų grandinė yra panaši į universalią duomenų struktūrą – tiesinį sąrašą. Kiekvienas blokas, kuriame saugome informaciją, turi dar rodyklę, kuri rodo į kaimyninį bloką (jo adresą kompiuterio atmintyje).



Tačiau rodyklė  $H()$  yra kriptografinė.

- ▶ Kiekviename bloke saugome ir jo duomenų (informacijos) santrauką – hash reikšmę. Ją apskaičiuojame du kartus iš eilės panaudodami SHA256 funkciją.  
Ši santrauka yra bloko unikalūs ID.

Tačiau rodyklė  $H()$  yra kriptografinė.

- ▶ Kiekviename bloke saugome ir jo duomenų (informacijos) santrauką – hash reikšmę. Ją apskaičiuojame du kartus iš eilės panaudodami SHA256 funkciją. Ši santrauka yra bloko unikalūs ID.
- ▶ Rodyklėje  $H()$  saugome kaimyninio (prieš tai buvusio) bloko santrauką. Šis kaimyno ID (santrauka) yra dalis informacijos, patalpintos naujame bloke.

- ▶ Taigi, jeigu bandysime pakeisti kažkurio bloko duomenis, tai pasikeis ir jo ID.



- ▶ Taigi, jeigu bandysime pakeisti kažkurio bloko duomenis, tai pasikeis ir jo ID.
- ▶ Norėdami paslėpti šį nusikaltimą, turime pakeisti ir po jo einančio bloko rodyklės informaciją  $H()$ . Tai pakeis ir šio bloko informacijos santrauką.

- ▶ Taigi, jeigu bandysime pakeisti kažkurio bloko duomenis, tai pasikeis ir jo ID.
- ▶ Norėdami paslėpti šį nusikaltimą, turime pakeisti ir po jo einančio bloko rodyklės informaciją  $H()$ . Tai pakeis ir šio bloko informacijos santrauką.
- ▶ Tęsdami procesą pasieksime visos blokų grandinės rodyklę, o jos pakeisti negalime (ji yra viešai publikuota).

- ▶ Taigi, jeigu bandysime pakeisti kažkurio bloko duomenis, tai pasikeis ir jo ID.
- ▶ Norėdami paslėpti šį nusikaltimą, turime pakeisti ir po jo einančio bloko rodyklės informaciją  $H()$ . Tai pakeis ir šio bloko informacijos santrauką.
- ▶ Tęsdami procesą pasieksime visos blokų grandinės rodyklę, o jos pakeisti negalime (ji yra viešai publikuota).
- ▶ Kol kas tarsime, kad egzistuoja toks Centras, kuriam patikėtas blokų grandinės rodyklės  $H()$  saugojimas. Vėliau parodysime, kad bitkoinų technologijoje Centras nenaudojamas, ši kriptovaliuta gyvuoja decentralizuotoje aplinkoje.

Transakcijos yra svarbiausia bitkoinų sudedamoji dalis.

Tai duomenų struktūra (nepamirškime, kad bitkoinai yra virtuali valiuta), kurioje užšifruota/užkoduota informacija apie tai, kokie mainai vykdomi tarp bitkoinų sistemos dalyvių.

Ši informacija yra talpinama ir saugoma **Buhalterinėje knygoje**, realizuotoje panaudojant blokų grandinę.

Svarbu susipažinti:

- ▶ koks yra transakcijos formatas;

Svarbu susipažinti:

- ▶ koks yra transakcijos formatas;
- ▶ kaip ji realizuojama,

Svarbu susipažinti:

- ▶ koks yra transakcijos formatas;
- ▶ kaip ji realizuojama,
- ▶ kaip patikrinamas transakcijos teisingumas/leistinumas,

Svarbu susipažinti:

- ▶ koks yra transakcijos formatas;
- ▶ kaip ji realizuojama,
- ▶ kaip patikrinamas transakcijos teisingumas/leistinumas,
- ▶ kaip ir kiek transakcijų yra saugoma viename transakcijų bloke.



Svarbu susipažinti:

- ▶ koks yra transakcijos formatas;
- ▶ kaip ji realizuojama,
- ▶ kaip patikrinamas transakcijos teisingumas/leistinumas,
- ▶ kaip ir kiek transakcijų yra saugoma viename transakcijų bloke.
- ▶ Vėliau aptarsime, kaip transakcijų blokas yra visiems laikams įrašomas į blokų grandinę ir apsaugomas nuo bet kokių kurios nors transakcijos pakeitimų.

Kokius svarbiausius pavojus galime prognozuoti ( šį sąrašą kviečiu papildyti savo variantais):

Visa informacija apie nepanaudotas monetas yra skelbiama viešai, ar galiu panaudoti man **nepriklausančius pinigus**?

Ar galiu atlikti dvigubą mokėjimą – t.y. ta pačia **SAVO** moneta apmokėti dvi skirtingas sąskaitas?

Ar galiu į Buhalterinę knygą įrašyti neteisingas transakcijas?

## Transakcijos gyvavimo ciklas

1. Transakcija sukūriama – nurodoma, kokias lėšas ji naudoja ir kaip šios lėšos bus paskirstytos.
2. Lėšų savininkai pasirašo/patvirtina šį paliepiimą (**kriptografiniais skaitiniais parašais**).
3. Patikrinus sukurtos transakcijos sudarymo teisingumą ir jos leistinumą, ji įtraukiama į blokų grandinę.
4. Naujieji lėšų savininkai gali jas naudoti, t.y. kurti naujas transakcijas.

# TRANSAKCIJOS STRUKTŪRA BLOKO VIDUJE:

1. Lėšų šaltinių skaičius (Input Counter) – iš kokių bitkoinų monetų sudaromas mokėjimas.
2. Lėšų šaltinių aprašai (Inputs) – kokioje transakcijoje ir kelintame jos pavedime (Output Counter) buvo paskirti pinigai.
3. Lėšų gavėjų skaičius (Output Counter)
4. Kam ir kiek skirta lėšų (Outputs)
5. Transakciją pasirašo visi sistemos dalyviai, kurie skiria savo lėšas (priminsime, kad skaitmeninio parašo būtina sudedamoji dalis yra pasirašančiojo viešasis raktas **pk**).

Labai svarbu suprasti, kad bitkoinų protokole **nėra** tokios sąvokos, kaip sistemos dalyvio sąskaitos balansas.

Blokų grandinėje **galime tik surasti** tas monetas ir jų vertes, kurių bitkoinų savininkai dar neišleido – jos vadinamos **UTXO** (unspent transaction output).

Jus turite tiek pinigų, kiek jų yra su Jūsų adresais susietose dar n panaudotose monetose, **kurias pripažįsta kiti tinklo dalyviai**.

1. Monetos vertė Satoshiais ( $10^{-8}$  BTC) 8 baitai
2. Pinigų užraktas (Locking Script) – nurodo sąlygas, kurias turi išpildyti tas, kas norės panaudoti lėšas.

Skripto tekstas gali reikšti tokį reikalavimą:

Pinigai yra skirti sistemai, kurio viešojo rakto santrauka yra *pkh* ir kuris gali savo transakciją patvirtinti skaitmeniniu parašu, atitinkančiu jo nurodytą viešąjį raktą *pk*.

<https://en.bitcoin.it/wiki/Transaction>

Input:

Previous tx:

f5d8ee39a430901c91a5917b9f2dc19d6d1a0e9cea205b009ca73dd04470b9a6

Index: 0

**scriptSig:**

304502206e21798a42fae0e854281abd38bacd1aedd3ee3738d9e1446618c4571  
d1090db022100e2ac980643b0b82c0e88ffdfec6b64e3e6ba35e7ba5fdd7d5d6c  
c8d25c6b241501

Output:

Value: 524300000

**scriptPubKey:** *OP\_DUP OP\_HASH160*

404371705fa9bd789a2fcd52d2c580b65d35549d

*OP\_EQUALVERIFY OP\_CHECKSIG*

Naujos transakcijos lėšų šaltinio patvirtinimas skaitmeniniu parašu:

scriptSig: `<sig> <pubKey>`

Informacija apie užrakto reikalavimus transakcijoje, kurioje buvo suformuotas šis šaltinis (bitkoino moneta):

scriptPubKey: `OP_DUP OP_HASH160 <pubKeyHash>  
OP_EQUALVERIFY OP_CHECKSIG`

Skriptai realizuojami panaudojant svarbiausią informatikoje duomenų struktūrą – [steką](#).



Unlocking Script  
(scriptSig)

+

Locking Script  
(scriptPubKey)

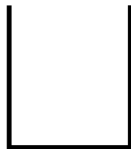
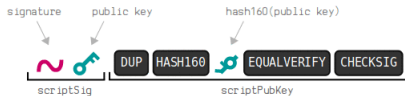
<sig> <PubK>

DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG

Unlock Script  
(scriptSig) is provided  
by the user to resolve  
the encumbrance

Lock Script (scriptPubKey) is found in a transaction output and is the  
encumbrance that must be fulfilled to spend the output

Standard Script: P2PKH



Stack

learnmeabitcoin.com

Standard Script: P2PKH



Stack

learnmeabitcoin.com



Standard Script: P2PKH



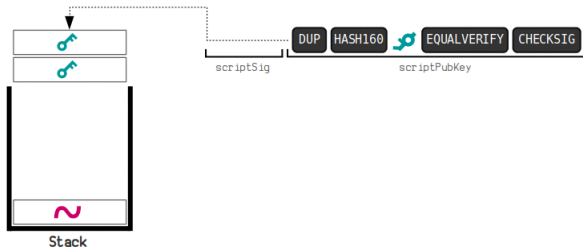
learnmeabitcoin.com

Standard Script: P2PKH



learnmeabitcoin.com

Standard Script: P2PKH



learnmeabitcoin.com

Standard Script: P2PKH



learnmeabitcoin.com

Standard Script: P2PKH



learnmeabitcoin.com

Standard Script: P2PKH



learnmeabitcoin.com

Standard Script: P2PKH



learnmeabitcoin.com

Standard Script: P2PKH



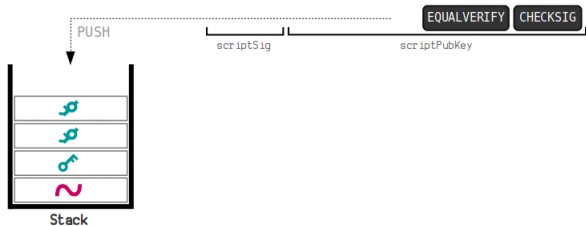
learnmeabitcoin.com



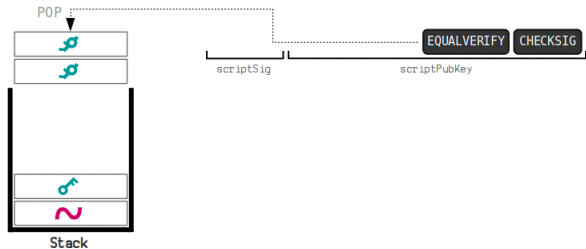
learnmeabitcoin.com



learnmeabitcoin.com



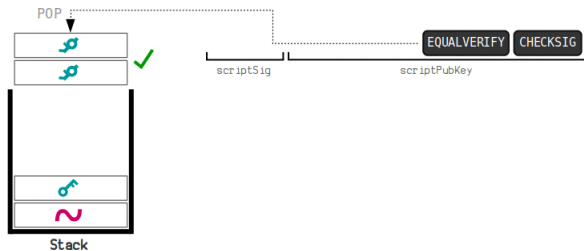
learnmeabitcoin.com



learnmeabitcoin.com

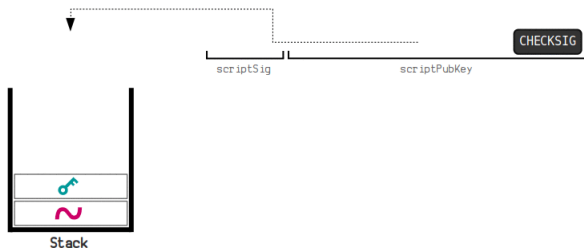


Standard Script: P2PKH



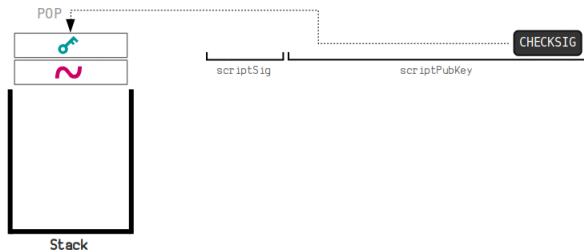
learnmeabitcoin.com

Standard Script: P2PKH



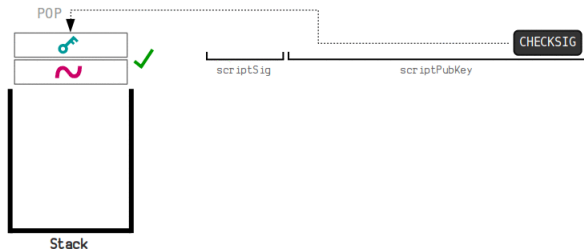
learnmeabitcoin.com

Standard Script: P2PKH

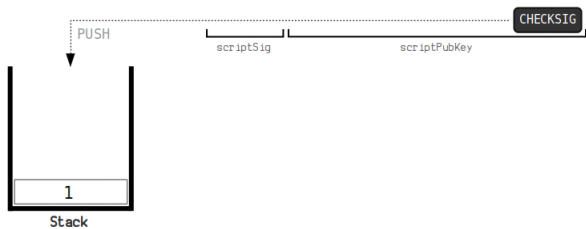


learnmeabitcoin.com

Standard Script: P2PKH



learnmeabitcoin.com

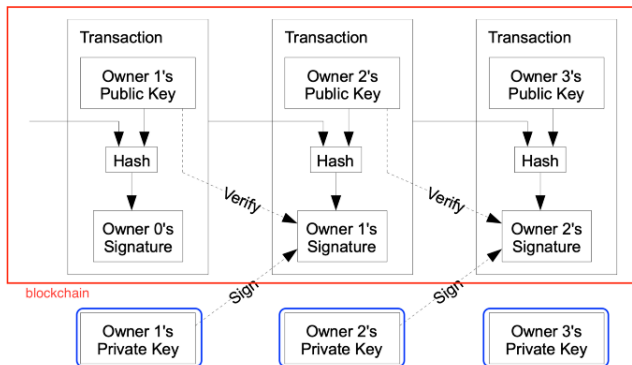


learnmeabitcoin.com



learnmeabitcoin.com

# TRANSAKCIJŲ GRANDINĖ

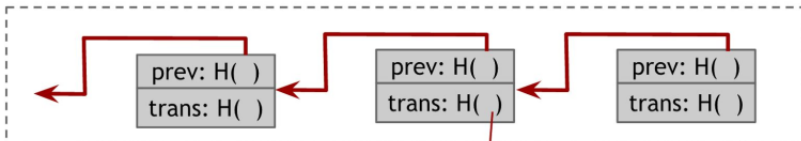


- ▶ Transakcijos saugomos blokuose, kiekvieno bloko dydis iki 1 MB.

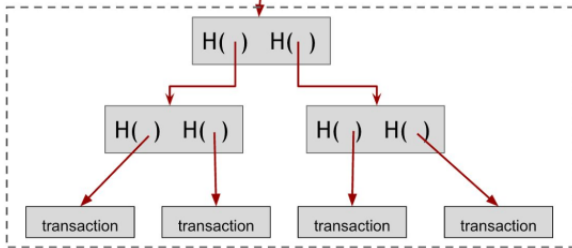
- ▶ Transakcijos saugomos blokuose, kiekvieno bloko dydis iki 1 MB.
- ▶ Viename bloke talpiname vidutiniškai 2200 transakcijų.

- ▶ Transakcijos saugomos blokuose, kiekvieno bloko dydis iki 1 MB.
- ▶ Viename bloke talpiname vidutiniškai 2200 transakcijų.
- ▶ Bloke transakcijos saugomos binarinio santraukų medžio duomenų struktūroje (hash tree arba Merkle tree)

Hash chain of blocks



Hash tree (Merkle tree) of transactions in each block





Pirmasis tokios sistemos elementas yra **Peer to Peer (P2P)** tinklas. Tinklo nariai yra sujungti internetu ir tiesiogiai bendrauja su nedideliu kiekiu "kaimynų". Tačiau per keletą tarpininkų jie gali perduoti informaciją **visiems** tuo metu tinkle esantiems nariams.

Tokio tinklo vartotojai yra **lygiaverčiai**, kiekvienas veikia ir kaip klientas, ir kaip serveris. Jie siunčia ir gauna bitkoinus nesinaudodami tarpininkų leidimais ar paslaugomis.

Blokų grandinė yra saugi, nes paskirstytame tinkle saugoma daug jos kopijų.

Nuolat vyksta narių kaita: vieni pasitraukia, kiti ateina.

Bitkoinų P2P tinkle naudojamas paskelbtasis kriptografinis protokolas ir jame atliekami visi mokėjimai.

**Visi sprendimai yra priimami konsensuso principu.**

Nėra jokio sinchronizacijos taško, bet garantuojama, kad per tam tikrą laiką šį sprendimą patvirtins visi tinklo nariai, t.y. jie vėl vykdo tą patį algoritmą ir saugo vienodas bloky grandines.

Antrasis sistemos saugumo ir decentralizacijos elementas grindžiamas algoritmu, kaip naujasis blokas yra įtraukiamas į bloką grandinę. Nenaudojama jokia (centralizuota) taisyklė, pasakanti, kurio tinklo nario parengtas naujas blokas bus įtrauktas.

- ▶ Reikia išspręsti sudėtingą matematinį uždavinį, kai vienintelis žinomas sprendimo būdas yra perrinkti visus variantus.

Antrasis sistemos saugumo ir decentralizacijos elementas grindžiamas algoritmu, kaip naujasis blokas yra įtraukiamas į blokų grandinę. Nenaudojama jokia (centralizuota) taisyklė, pasakanti, kurio tinklo nario parengtas naujas blokas bus įtrauktas.

- ▶ Reikia išspręsti sudėtingą matematinį uždavinį, kai vienintelis žinomas sprendimo būdas yra perrinkti visus variantus.
- ▶ Prie bloko metadatos informacijos prijungiamas papildomas stringas, (**nonce**), kurio ilgis 32 bitai. Keisdami šiuos bitus turime surasti tokią jo reikšmę, kad viso bloko santrauka būtų mažesnė už nurodytą slenkstinę reikšmę **target**. Tokia santrauka turi prasidėti nurodytu skaičiumi nuliių.

- ▶ Didėjant tinklo skaičiavimo pajėgumams, tenka padidinti pasirenkamų bitų skaičių, nes 32 bitų neužtenka, kad uždavinio sprendimo laikas būtų 10 minučių (tam reikia daugiau nei 60 bitų).

- ▶ Didėjant tinklo skaičiavimo pajėgumams, tenka padidinti pasirenkamų bitų skaičių, nes 32 bitų neužtenka, kad uždavinio sprendimo laikas būtų 10 minučių (tam reikia daugiau nei 60 bitų).
- ▶ Papildomą **Extra nonce** rekomenduojama užduoti coinbase transakcijoje.

- ▶ Didėjant tinklo skaičiavimo pajėgumams, tenka padidinti pasirenkamų bitų skaičių, nes 32 bitų neužtenka, kad uždavinio sprendimo laikas būtų 10 minučių (tam reikia daugiau nei 60 bitų).
- ▶ Papildomą **Extra nonce** rekomenduojama užduoti coinbase transakcijoje.
- ▶ Uždavinio sudėtingumas koreguojamas kiekvieną kartą, kai į tinklą įtraukiami 2016 naujų blokų (maždaug, kas 14 dienų). Jeigu vidutinis vieno bloko generavimo laikas buvo mažesnis nei 10 minučių, tai padidinamas matematinio uždavinio sudėtingumas, priešingu atveju - sumažinamas.

- ▶ Sprendimo metu naudojami resursai (elektra, kompiuteriai), taigi naujo bloko generavimas kainuoja pakankamai brangiai.



- ▶ Sprendimo metu naudojami resursai (elektra, kompiuteriai), taigi naujo bloko generavimas kainuoja pakankamai brangiai.
- ▶ Todėl sukurtas dar vienas išradingas ir efektyvus bitkoinų tinklo elementas – kasėjai yra skatinami piniginiu prizu. Už kiekvieną parengtą ir įtrauktą į blokų grandinę bloką kasėjui išmokama fiksuota naujų bitkoinų vertė (šiuo metu ji lygi 6.25 BTC).

- ▶ Sprendimo metu naudojami resursai (elektra, kompiuteriai), taigi naujo bloko generavimas kainuoja pakankamai brangiai.
- ▶ Todėl sukurtas dar vienas išradingas ir efektyvus bitkoinų tinklo elementas – kasėjai yra skatinami piniginiu prizu. Už kiekvieną parengtą ir įtrauktą į blokų grandinę bloką kasėjui išmokama fiksuota naujų bitkoinų vertė (šiuo metu ji lygi 6.25 BTC).
- ▶ Naują parengtą bloką patikrina visi tinklo dalyviai ir jį prijungia prie "ilgiausios" turimos blokų grandinės. "Ilgiausia" grandinė yra ta, kurios generavimui reikėjo skirti daugiausia skaičiavimų (ji nebūtinai sudaryta iš didžiausio skaičiaus blokų, nors dažniausiai taip ir yra).

Nodes will adopt this chain because it took more work to build.

Difficulty = 4

Difficulty = 1



Alternative chain.

Difficulty = 1

Difficulty = 1



# SKAIČIAVIMO EKSPERIMENTO REZULTATAI

Pasirinkome slenkstinę reikšmę  $m = 5$  nulius.

Patikrinome  $10^8$  nonce elementų.

Skaiciavimo laikas 2.5 minutės, suradome 95 laimėtojus.

Testų skaičius iki naujo laimėtojo radimo

$c_{min} = 11741$ ,  $c_{max} = 5599570$ , t.y. gali skirtis 50 kartų.

Pasirinkome sudėtingesnę slenkstinę reikšmę  $m = 6$ .

Patikrinome  $2 \cdot 10^8$  nonce elementų.

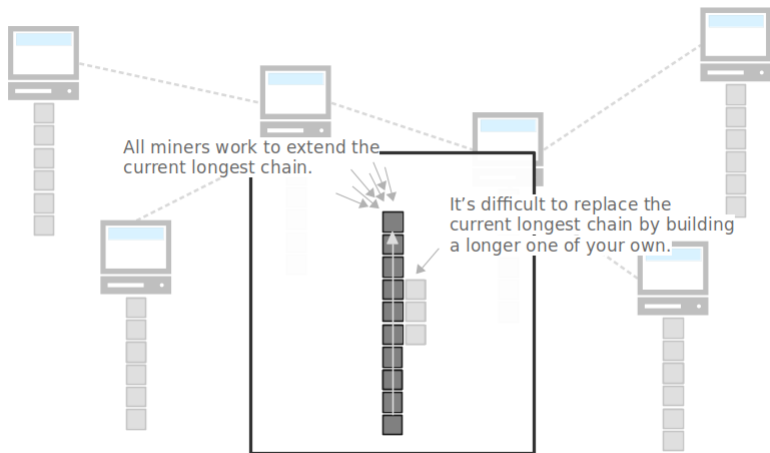
Skaiciavimo laikas 5 minutės, suradome 10 laimėtojų.

Testų skaičius iki naujo laimėtojo radimo

$c_{min} = 1657862$ ,  $c_{max} = 67186208$ , t.y. gali skirtis 40 kartų.

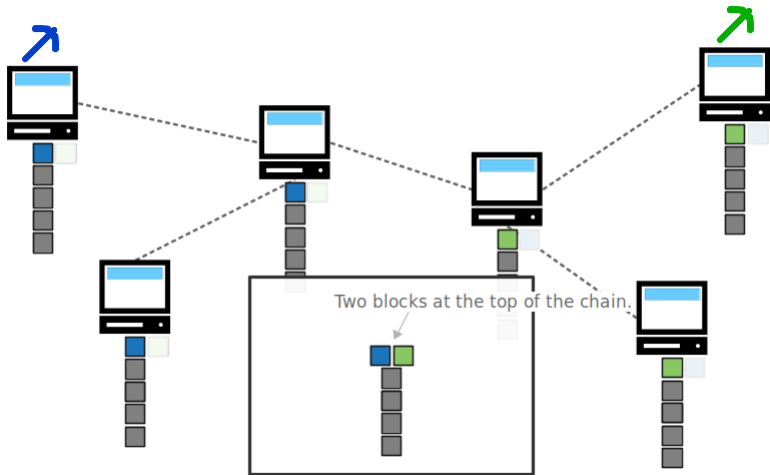
Tarp surastų laimėtojų nebuvo nei vieno, kurio santrauka prasideda 7 nuliais.

Matematinio uždavinio sudėtingumas ir "ilgiausios" blokų grandinės taisyklė patikimai apsaugo grandinę nuo bandymų pakeisti anksčiau įtrauktų blokų turinį ar juos pašalinti iš grandinės.

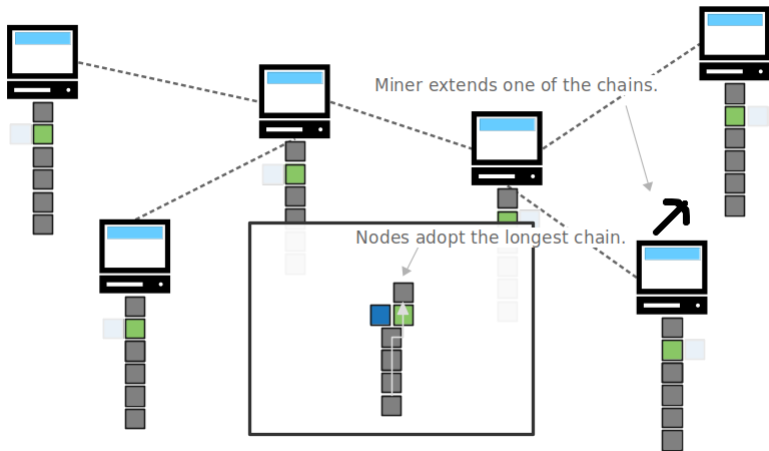


- ▶ Kasėjas, prieš pradėdamas generuoti naują bloką, į hash rodyklę turi įtraukti pasirinkto bloko santrauką. Remiantis protokolu racionalu pratęsti "ilgiausią" grandinę, tai padidina jo šansus lenktynėse.  
Vienoks ar kitoks pasirinkimas paveikia matematinio uždavinio sprendimą. Vėliau pakeisti bloką galime tik atlikę papildomus ilgus skaičiavimus ir beveik garantuotai pralaimėję konkurentams.

- ▶ Kasėjas, prieš pradėdamas generuoti naują bloką, į hash rodyklę turi įtraukti pasirinkto bloko santrauką. Remiantis protokolu racionalu pratęsti "ilgiausią" grandinę, tai padidina jo šansus lenktynėse.  
Vienoks ar kitoks pasirinkimas paveikia matematinio uždavinio sprendimą. Vėliau pakeisti bloką galime tik atlikę papildomus ilgus skaičiavimus ir beveik garantuotai pralaimėję konkurentams.
- ▶ Aišku, kad tinkle trumpai gali egzistuoti kelios skirtingos blokų grandinės, bet pakankamai greitai vėl pasiekiamas visų dalyvių konsensusas.







- ▶ Kasėjai yra suinteresuoti įtraukti naują bloką į ilgiausią grandinę, nes užmokestį už bloko generavimą jie gauna tik tada, kai jų blokas patvirtinamas 100 naujų blokų įtraukimu į grandinę (maždaug po 17 valandų).

- ▶ Kasėjai yra suinteresuoti įtraukti naują bloką į ilgiausią grandinę, nes užmokestį už bloko generavimą jie gauna tik tada, kai jų blokas patvirtinamas 100 naujų blokų įtraukimu į grandinę (maždaug po 17 valandų).
- ▶ Tinklo dalyviams rekomenduojama palaukti, kol atliktas mokėjimas bus patvirtintas blokų grandinėje 6 naujais blokais ir tik tada teikti prašomą paslaugą ar prekes (maždaug po 1 valandos).

- ▶ Kasėjai yra suinteresuoti įtraukti naują bloką į ilgiausią grandinę, nes užmokestį už bloko generavimą jie gauna tik tada, kai jų blokas patvirtinamas 100 naujų blokų įtraukimu į grandinę (maždaug po 17 valandų).
- ▶ Tinklo dalyviams rekomenduojama palaukti, kol atliktas mokėjimas bus patvirtintas blokų grandinėje 6 naujais blokais ir tik tada teikti prašomą paslaugą ar prekes (maždaug po 1 valandos).
- ▶ **Sėkmingo atsiskaitymo virtualiosiomis valiutomis!**

- ▶ Kasėjai yra suinteresuoti įtraukti naują bloką į ilgiausią grandinę, nes užmokestį už bloko generavimą jie gauna tik tada, kai jų blokas patvirtinamas 100 naujų blokų įtraukimu į grandinę (maždaug po 17 valandų).
- ▶ Tinklo dalyviams rekomenduojama palaukti, kol atliktas mokėjimas bus patvirtintas blokų grandinėje 6 naujais blokais ir tik tada teikti prašomą paslaugą ar prekes (maždaug po 1 valandos).
- ▶ Sėkmingo atsiskaitymo virtualiosiomis valiutomis!
- ▶ Sėkmingo bitkoinų kasimo!!!