Raspodijeljene glavne knjige i kriptovalute

Pohrana i upotreba Bitcoina

Stjepan Begušić, Ante Đerek, Zvonko Konstanjčar

16. studenoga 2023.

Ponavljanje: Alternativni pristupi rudarenju

Glavni problemi proof-of-work sustava:

- Ogromna potrošnja energije
- Rudarenje se svelo na nekoliko velikih bazena (ASIC) - sebično rudarenje

Alternativni pristupi rudarenju

- Slagalice otporne na ASIC
- Proof-of-Useful-Work
- Proof-of-Stake i virtualno rudarenje

Ponavljanje: vrijednost Bitcoina

Tri važne povezane ideje oko Bitcoina - cirkularna ovisnost

- Sigurnost sustava kriptovalute ovisi o rudarenju
- Rudarenje ovisi o vrijednosti kriptovalute
- Vrijednost kriptovalute ovisi o sigurnosti sustava

Danas..

Pitanje za danas: Kako pohranjujemo i koristimo Bitcoine u praksi?

Sadržaj

- Jednostavna lokalna pohrana
- Hladna i topla pohrana
- Podjela i tajno dijeljenje ključeva
- Online novčanici i burze
- Usluge plaćanja Bitcoinom
- Ekonomija tržišta kriptovaluta

Jednostavna lokalna pohrana

Najjednostavniji način pohrane Bitcoina je na lokalni uređaj.
Da bi potrošili Bitcoine trebamo imati:

- Javne informacije - adresu novčića
- Privatne informacije - privatni ključ vlasnika novčića

Definicija

Pohrana Bitcoina je postupak pohrane i upravljanja privatnim ključevima.

Različiti pristupi upravljanju ključevima nude različite kompromise između:

- Dostupnosti - mogućnost da potrošite novčiće kad to trebate/želite
- Sigurnosti - nitko drugi ne smije moći potrošiti vaše novčiće
- Praktičnosti - jednostavnost upotrebe

Jednostavna lokalna pohrana

Jednostavna metoda za upravljanje ključem: pohrana u datoteku na lokalnom uređaju

- Praktično
- Nije nužno dostupno - dostupno je koliko i vaš uređaj
- Nije nužno sigurno - sigurno je koliko i vaš uređaj

Pohrana ključa na mobitel je slično nošenju novca u novčaniku

- Većina ljudi se ne brine ako ima 100 kuna u novčaniku
- Većina ljudi bi bila zabrinuta ako nosi u novčaniku novce za kupnju stana

Novčanici

Za lokalnu pohranu ključeva obično se koriste "novčanici".

Definicija

Novčanik je softver koji sprema informacije o svim novčićima, upravlja detaljima oko ključeva te olakšava korištenje kriptovaluta s prikladnim korisničkim sučeljem.

Za razmjenu Bitcoina treba nam razmjena adresa.

Razmjena adresa uobičajeno se radi:

- Tekstualni zapis (baza 58)
- QR kod - novčanik sam pretvara u niz koji predstavlja Bitcoin adresu

Pogotovo korisno u upravljanju adresama i ključevima - u pravilu za svaki novčić (UTXO) želimo koristiti novu adresu.

Razmjena adresa

`1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa`

The address that received the very first Bitcoin block reward in the genesis block, base58 encoded.

Izvor: `bitcoinbook.cs.princeton.edu`

Vanity adrese

Definicija

Vanity adresa je adresa u kojoj je određeni segment unaprijed definiran.

Primjer: FER3kq56YuERTr7U8Pu7TYJKre35d3TRXb

- Postoje alati za njihovo generiranje
- Za k definiranih znakova - potrebno je generirati u prosjeku 58^k adresa
- Za FER3 potrebno je generirati u prosjeku milijun adresa

Hladna i topla pohrana

Topla pohrana (*engl. hot storage*)

- Spremanje Bitcoina na osobne uređaje
- Praktično, ali riskantno

Hladna pohrana (*engl. cold storage*)

- Spremanje Bitcoina udaljeno (offline)
- Manje praktično, ali sigurnije

- Ako se koriste hladna i topla pohrana, potrebno je imati različite privatne ključeve
- Želimo prebacivati sredstva iz jednog spremišta u drugo - svaka strana mora znati adresu druge strane
- **Potencijalni problem** - ako želimo kod svakog prebacivanja koristiti novu adresu na hladnoj strani

Hijerarhijski novčanici

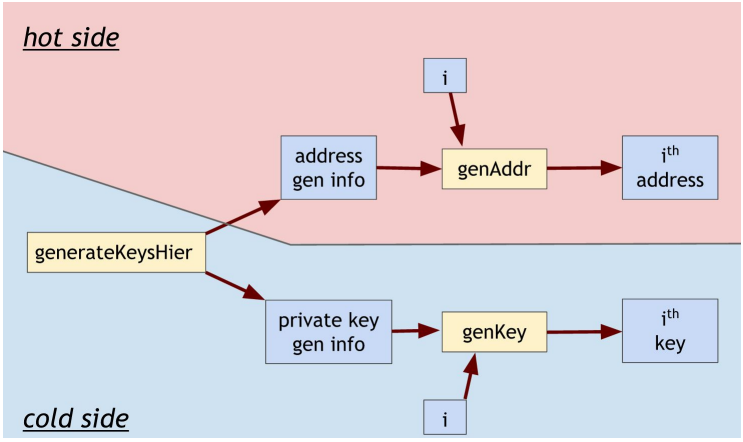
Definicija

Hijerarhijski novčanik je skup novčanika kod kojeg hladna strana ima proizvoljno adresa te topla strana zna za te adrese kroz jednu kratku komunikaciju između dvije strane.

Idejno rješenje

- Klasično adrese generiramo preko funkcije generateKeys (output: javni ključ i privatni ključ)
- Ovdje generiramo (preko funkcije generateKeysHier):
  - umjesto jedne adrese - address generation info
  - umjesto jednog privatnog ključa - key generation info
- Rezultat je niz adresa i odgovarajućih privatnih ključeva
  - adresa(i) = generateAddress(address generation info, i)
  - privatni ključ(i) = generateKey(key generation info, i)

Hijerarhijska struktura



Izvor: `bitcoinbook.cs.princeton.edu`

Hijerarhijska struktura

- Sve varijante digitalnih potpisa ne podupiru nužno hijerarhijske strukture, ali ECDSA koji koristi Bitcoin da.
- Dvije razine sigurnosti (topla i hladna pohrana) mogu se proširiti na više razina
- Svojstvo nepovezivosti adresa: nitko ne može znati da su adrese generirane iz istog novčanika
- Pitanje: kako pohraniti ključeve u hladnoj pohrani?
  - Na sigurne uređaje (npr. računalo ili prijenosnu memoriju)
  - Fizička sigurnost: Držati ih u sefu?
  - Dostupnost?

Novčanici zasnovani na frazi

Pristup Bitcoinima se kontrolira korištenjem tajne fraze (zgodno kada se negdje putuje).

Idejno rješenje

- Treba nam **algoritam** koji transformira frazu u javni i privatni ključ na deterministički način
- Primjer
  - Hash funkcijom iz fraze možemo generirati privatni ključ
  - Standardnim postupcima iz privatnog ključa možemo dobiti javni ključ
  - Kombiniranjem s idejom hijerarhijskih novčanika možemo dobiti čitav skup javnih i privatnih ključeva
- Problem ako napadač otkrije frazu - čitava sigurnost se temelji na tome.

Pogađanje fraze nije usmjereno na pojedinog korisnika i ne ostavlja trag

Ostali načini spremanja ključeva

Papirnati novčanici

- Možemo isprintati ključ i spremiti ga na tajno mjesto
  - Kao QR kod
  - Kao zapis u bazi 58

Specijalizirani protuprovalni uređaji

Uređaji obično traže šifru ili traže odgovore na neka pitanja.

- Ključevi se mogu spremiti u te uređaje, ili
- Uređaji mogu generirati ključeve

Podjela i dijeljenje ključeva

Do sada smo cjeloviti ključ spremali na jedno mjesto - *single point of failure*.

Problem

- Netko napadne to mjesto
- Nastanak kvara

Zadatak

Možemo li napraviti backup? Kako to utječe na sigurnost?

Izazov

Možemo li istovremeno povećati dostupnost i sigurnost?

Tajno dijeljenje

Ideja

- Želimo ključ S podijeliti na N dijelova
- Ako znamo bilo kojih K od tih N dijelova - tada možemo rekonstruirati ključ
- Ako znamo manje od K dijelova - tada nam to nimalo ne pomaže u otkrivanju ključa

Zadatak

Možemo li naprosto ključ podijeliti u dijelove?

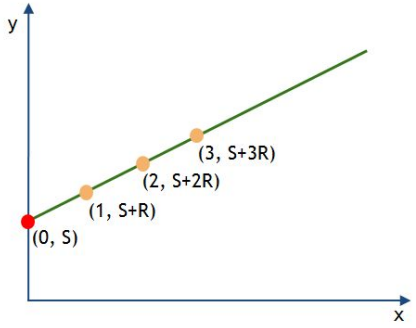
Tajno dijeljenje

Primjer N=2, K=2

- Generiramo slučajni broj R i iz njega $S \oplus R$
- Podijelimo ključ R i ključ $S \oplus R$ (logički XOR) kao dva dijela
- Znanje pojedinog dijela ne pomaže nam u rekonstrukciji S
- Kad primijenimo XOR na oba dijela dobijemo ključ S

Ova tehnika funkcionira dok god su N i K isti - kad je $N > K$ trebamo drukčije tehnike.

Tajno dijeljenje



Izvor: `bitcoinbook.cs.princeton.edu`

Slučaj $K = 2$, $N > K$

- S - tajna kodirana kao veliki cijeli broj, R - slučajan broj
- Bilo koje dvije narančaste su dovoljne za određivanje crvene
- Jedna narančasta ne nosi nikakvu informaciju o crvenoj

Algoritam

- P - veliki prosti broj
- Uvjeti: S i R moraju biti između 0 i $P-1$
- Točke generiramo
  - $x = 1, y = (S + R) \mathrm{mod} P$
  - $x = 2, y = (S + 2R) \mathrm{mod} P$
  - itd.
- Tajna odgovara točki $x = 0, y = S$ - možemo je dobiti iz

Tajno dijeljenje

- Za slučaj $K > 2$ potreban polinom reda $K - 1$
- Broj točaka potrebnih za reproducirati S je red polinoma $+1$

Svojstva tajnog dijeljenja:

- Dijelimo privatni ključ na N dijelova koje možemo spremiti na N različitih uređaja
- **Ako bilo tko ukrade jedan uređaj** - nema nikakvu informaciju o ključu
- **Ako neki uređaji prestanu raditi** - ključ je i dalje sačuvan

Problem

Nismo u potpunosti eliminirali "*single point of failure*".

- Postoji točka u kojoj se dijelovi spajaju u svrhu izračuna ključa.

Idejno rješenje

Ako su dijelovi spremljeni na različitim uređajima - možemo odrediti ključ na necentraliziran način. Primjer: novčanik s dvorazinskom sigurnošću $K = N = 2$.

- Npr. iniciranje plaćanja se može pokrenuti na računalu
- Računalo šalje parcijalni potpis na mobitel
- Na mobitelu se javlja alarm s podatcima o plaćanju (primatelj, iznos, itd.) i traži se potvrda
- Ako je sve u redu, korisnik potvrđuje plaćanje i mobitel završava potpis koristeći svoj dio privatnog ključa te šalje transakciju u lanac blokova

Višestruki potpisi

Alternativni pristup "*single point of failure*" problemu.

Primjer

Martina, Marta, Marina, Mirela i Mirjana osnovale su kompaniju koja rudari Bitcoine 2012. godine te danas imaju na računu puno Bitcoina.

- Svaka od njih generira po jedan par privatni-javni ključ
- Svaka svoj privatni ključ štiti na poseban način
- Hladnu pohranu štite s tri od pet ključeva - da bi transakcija bila validna mora biti potpisana s tri od pet ključeva
- Ako napadač ukrade ključ od dvije osobe nije problem
- Ako dvije osobe izgube ključ nije problem

VAŽNO: Ovo nam direktno omogućuju Bitcoin skripte te nije poseban rezultat kriptografije.

Online novčanici

Definicija

Online novčanik je novčanik kod kojeg su informacije spremljene u oblaku te se njemu pristupa preko web preglednika ili aplikacija na mobitelu.

Prednosti i nedostaci u odnosu na lokalnu pohranu

- Velika prednost je praktičnost
  - Ne treba ništa instalirati na računalo
  - Na mobitelu se jednom instalira aplikacija
  - Ne treba spremati lanac blokova
  - Istom novčaniku možemo pristupati s više uređaja
- Postoje određeni sigurnosni problemi - mora postojati povjerenje u osobe i opremu

Poslovanje banaka

- Klijenti uplaćuju u banku depozite
- Banka kroz ugovore klijentima jamči da će im vratiti depozite u nekom trenutku (obično uz kamate)
- U međuvremenu banka te novce investira
- Centralne banke prisiljavaju komercijalne banke da dio tih novaca ne investiraju - obvezna pričuva

Definicija

Obvezna pričuva jest obveza kreditnih institucija da određeni postotak primljenih sredstava (primljeni a vista i oročeni depoziti, primljeni krediti i sl.) drže na računima kod centralnih banaka

U Hrvatskoj trenutno 12%, u EU oko 1%, a neke zemlje poput Australije, Švedske ih nemaju.

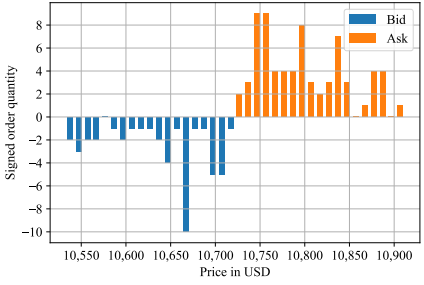
Obvezne pričuve - monetarni multiplikator

Obvezna pričuva omogućuje kontrolu nad ponudom novca te posljedično osiguranje monetarne stabilnosti i likvidnosti bankovnog sustava te neometano odvijanje platnog prometa. (Izvor: HNB)

Banka	Novi depoziti	Mogući zajmovi	Obvezne pričuve
1	100 000	90 000	10 000
2	90 000	81 000	9 000
3	81 000	72 900	8 100
4	72 900	65 610	7 290
5	65 610	59 049	6 561
Ostatak	590 490	531 441	59 049
Ukupno	1 000 000	900 000	100 000

Bitcoin burze - poslovanje slično bankama

- Klijenti uplaćuju depozite u obliku Bitcoina ili fiat valuta
- Burze jamče da će vratiti depozite kada to klijenti zatraže
- Burze nude razne funkcije koje inače nude i banke - npr. plaćanja u Bitcoinima (u oba smjera)
- Nude usluge trgovanja - Bitcoin vs. fiat valute
  - Obično to rade po principu direktnog spajanja
  - "Sparuju" klijente sa suprotnim zahtjevima



Trgovina na burzama

Ako se na burzi dogodi transakcija (kupnja-prodaja) to ne znači da se dogodila transakcija na lancu blokova.

- Transakcije na burzama se uglavnom ne propagiraju na lanac blokova.
- Mijenjaju se samo stanja na računima klijenata (obećanja)

Burze imaju pozitivnih i negativnih strana.

Glavna pozitivna strana je što povezuju na jednostavan način kriptovalute s realnim svijetom kroz trgovinu s fiat valutama.

Rizici

Prisutni su slični rizici kao i kod poslovanja s bankama

- Rizik navala na banke/burze (*engl. bank run*)
  - veliki broj ljudi u istom trenutku zatraži isplatu
  - problem su (dez)informacije
- Rizik prevare od strane vlasnika burze (Ponzi shema)
  - na neki način se klijentima obećaju veliki povrati u budućnosti
  - dio klijenata u početku dobije te povrate od drugih koji uplaćuju
- Sigurnosni rizici
  - napadi izvana - netko upadne u sustav
  - napadi iznutra - djelatnik burze uvidi i iskoristi priliku

Svi ovi rizici su se realizirali! Pitanje je štiti li tko klijente burze?

Banke

- Centralne banke (HNB) nadziru komercijalne banke, npr. kroz obavezne pričuve
- Vlade često kroz agencije i zakone reguliraju u što banke smiju ulagati
  - Vlade ponekad osiguravaju dio depozita banaka
  - Vlade ponekad spašavaju banke

Tržišta kapitala

- Trgovanje dionicama i obveznicama, preko pouzdanih softverskih platformi (Xetra, Euronext)
- Efikasnost tržišta ovisna o veličini (dnevni volumen ZSE: 10 mil. HRK, NYSE: 30 mlrd. USD)
- Regulirane državnim agencijama (HANFA, SEC), strogo zabranjeni pokušaji manipulacije:
  - "pump & dump"
  - "spoofing"
  - "wash trading"
- Investitori trguju isključivo preko brokera, a odvojene agencije (SKDD) obavljaju tzv. "clearing"

Tržišta valuta

- Nije centralna burza, već skup dionika i aktera (centralne banke, tvrtke, brokeri za male investitore)
- Najveće, najefikasnije i najlikvidnije tržište na svijetu (dnevni volumen 5 bil. USD)
- Zbog visokog volumena i efikasnosti jako teško moguće manipulacije

Tržišta kriptovaluta

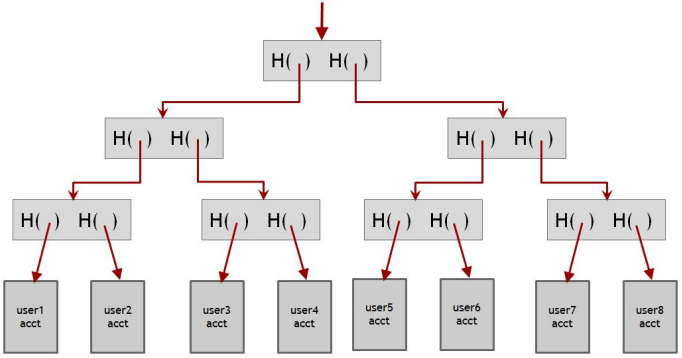
- Uglavnom neregulirane burze, relativno neefikasne (velike mogućnosti arbitraže)
- Zbog manjka regulacije poznati primjeri manipulacija:
  - "pump & dump" organizacije: https://bitfalls.com/2018/01/12/anatomy-pump-dump-group/
  - Lažni "spoof" nalozi na Bitfinex-u: https://hackernoon.com/meet-spoofy-how-a-single-entity-dominates-the-price-of-bitcoin-39c711d28eb4
  - Neke burze prijavljuju lažno napuhane volumene: https://www.blockchaintransparency.org/november-2018-report/
  - 20% volumena na Coinbase-u je njihovo vlastito trgovanje https://www.coindesk.com/new-york-ags-office-takes-aim-at-crypto-exchanges-in-new-report/
  - Rad objavljen u Journal of Monetary Economics o manipulaciji cijenom na Mt. Gox 2013 https://www.sciencedirect.com/science/article/abs/pii/S0304393217301666

Proof-of-reserve

Kriptografski "trik" kojim burze mogu svojim klijentima ponuditi dokaz o tome koliko imaju depozita - cilj je pokazati klijentima da postoji obavezna pričuva.

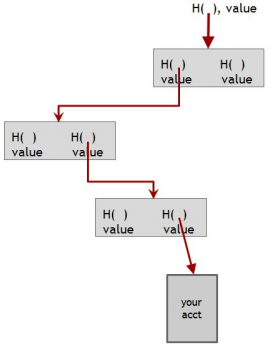
- Trebaju pokazati koliko imaju položenih depozita - transakcija sami sebi - **relativno lagano**
- Trebaju pokazati kolika imaju potraživanja za depozitima - proof-of-liabilities - **dosta teško**
  - ako se ne vodi računa o privatnosti onda se mogu objaviti informacije svih klijenata: username i iznos
  - ako nekoga preskočimo, postoji šansa da će nas razotkriti
  - postoji opasnost da se tu pojave lažni korisnici
  - potraživanja sigurno nisu veća
  - bolja varijanta organizirati klijente i Merkleovo stablo

Bitcoin burze - proof-of-liabilities



Izvor: `bitcoinbook.cs.princeton.edu`

Bitcoin burze - proof-of-liabilities



Izvor: `bitcoinbook.cs.princeton.edu`

Platne usluge

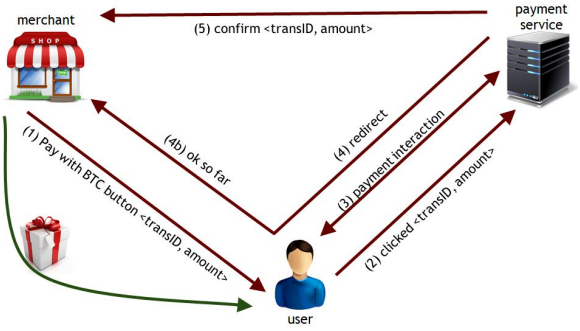
Razmatramo kako online i klasične trgovine mogu poslovati s Bitcoinima.

Potrebe trgovina

- Svoje proizvode i usluge staviti na raspolaganje što većem broju kupaca
- Često ne žele imati Bitcoine na kraju dana, nego odgovarajuće fiat valute
- Traže jednostavan način za to - bez prevelikog razmišljanja o tehnologiji
- Niske razine rizika su uvjet za uspješnu implementaciju
  - rizik funkcioniranja nove tehnologije
  - sigurnosni rizici rada s Bitcoinima
  - tečajni rizici

Platne usluge postoje kako bi se zadovoljile potrebe **kupaca** i **prodavača**.

Platne usluge - pozadina



Izvor: `bitcoinbook.cs.princeton.edu`

1. Kupac odabere plaćanje s BTC te dobije transID i iznos
2. Kupac potvrđuje plaćanje s BTC te se transID i iznos šalju PS
3. PS pokreće plaćanje i rezultat je uplata BTC na adresu
4. PS obavještava kupca i trgovca da je uplata inicijalno OK
5. PS šalje direktno potvrdu da je sve OK i ide isporuka proizvoda

Platne usluge

Kraj kupnje završava

- Kada pružatelj platnih usluga šalje novac (npr. kune) trgovcu, pri čemu zadržava mali dio kao naknadu
- Sama namira se događa u nekim periodičkim intervalima, npr. jednom dnevno

Na kraju su svi zadovoljni

- Kupci imaju proizvod i platili su Bitcoinima
- Trgovine su prodale proizvod i imaju fiat valute

Platne usluge preuzimaju sav rizik

- Sigurnosni rizik - moraju imati dobre sigurnosne procedure
- Tečajni rizik - posebno problematično ako cijene Bitcoina jako fluktuiraju

Platne usluge

Uobičajeno posluju na velikim volumenima

- Primaju velike količine Bitcoina
- Plaćaju velike količine fiat valuta

Platne usluge su aktivni sudionici na burzama

- Imaju stalnu potrebu za trgovanjem
- Posebno im je važna likvidnost

Ekonomija tržišta kriptovaluta

Ponuda i potražnja

- Tržište je relativno veliko - umjerene količine Bitcoina se mogu kupiti i prodati u svakom trenutku
- Cijena je posljedica odnosa ponude i potražnje

Ponuda Bitcoina

- Ukupna količina Bitcoina koji se mogu kupiti
- 2023. u opticaju ima 19.5 milijuna, maksimum je 21 milijun.
- Rezerve burzi i svakodnevni priljev izrudarenih Bitcoina

Potražnja za Bitcoinima

- Bitcoin kao platežno sredstvo (posredovanje u transakcijama)
- Bitcoin kao investicija

Jednostavni model tržišnog ponašanja - oznake

- V_p - ukupna vrijednost transakcija u kojoj Bitcoin služi kao platežno sredstvo (mjerimo u USD po sekundi)
- δ - interval vremena u sekundama u kojem su Bitcoini izvan tržišta kako bi posredovali u transakciji (vrijeme od kupnje na jednoj strani do prodaje na drugoj strani)
- S_p - ukupna ponuda Bitcoina koja je raspoloživa kao platežno sredstvo (svi Bitcoini koji trenutno postoje umanjeni za Bitcoine koji služe kao dugoročna investicija)
- P - cijena Bitcoina u USD

Jednostavni model tržišnog ponašanja

- Strana ponude: koliko Bitcoina postaje dostupno svake sekunde za potrebe transakcija - u prosjeku $\frac{S_p}{\delta}$ Bitcoina svake sekunde ulazi na tržište
- Strana potražnje: Koliko Bitcoina po sekundi treba da bi se provele sve transakcije
  - V_p USD nam treba za posredovanja u transakcijama po sekundi
  - $\frac{V_p}{P}$ BTC nam treba za posredovanja u transakcijama po sekundi
- U ravnoteži: $\frac{S_p}{\delta} = \frac{V_p}{P} \rightarrow P = \frac{\delta}{S_p} V_p$
- Ako se plaćanje u BTC udvostruči - cijena BTC bi se trebala udvostručiti.

Za realističniji model trebalo bi uzeti u obzir dinamiku investicijskog dijela