Bitcoin
društvo Slovenije

Razkoli odprtih sistemov

Bitcoin VS BitcoinCash

24.09.2024, Kavarna Sputnik
Meetup XXXIV
Klemen Končan Verstovšek

»Bitcoinerji so pripadniki verske sekte«

1. Vera = protokol za prenos etičnih vrednot
2. Denar = protokol za prenos vrednosti
3. Jezik = internet = protokol za prenos informacij o vrednotah in vrednostih

Agenda

1. Veliki razkol krščanstva
2. Blocksize War

Krščanstvo

Osrednja vera zahodne civilizacije

Ozadje

Stara zaveza

- Skupno sveto pismo judovske in krščanske vere
- Prerokbe o prihodu odrešitelja:
- rojen v Betlehemu deviški materi
- bo izdan za 30 kosov srebra
- vladal potomcem Jakoba (Izraelu)
- Izničil zlo na Zemlji

JEZUS KRISTUS

- Jezusovo rojstvo je povzročilo razkol judovsko-krščanske vere
- Judje so Jezusa označili za lažnivca in lažnega preroka
- Judež Iškarijot je Jezusa izdal oblastem v zameno za 30 srebrnikov
- Rimski upravitelj Judeje, Poncij Pilat, je Jezusa obsodil na usmrtitev zaradi “izdajanja za judovskega kralja”
- Ecce, homo!

RAZKOL JUDOVSKE IN KRŠČANSKE VERE

- Razkol se je odvil v prvem stoletju n.št.
- Razlog: nasprotujoči pogledi na rojstvo, življenje, smrt in preporod Jezusa
- Rezultat: hardfork med dvema religijama
- Posledica: Razvoj Nove zaveze in razcvet krščanstva & razdrobitev judov po Evropi

NICEJSKO-CARIGRAJSKA VEROIZPOVED

- Osrednja vera/veroizpoved/molitev krščanske vere, danes del svete maše
- Sprejeta na prvem Ekumenskem koncilu v Niceji l. 325
- Dopolnjena na Ekumenskem koncilu v Carigradu l. 381

Verujem v enega Boga, Očeta vsemogočnega, stvarnika nebes in zemlje, vseh vidnih in nevidnih stvari.

In v enega Gospoda Jezusa Kristusa, edinorojenega Sina Božjega, ki je iz Očeta rojen pred vsemi veki in je Bog od Boga, Luč od Luči, pravi Bog od pravega Boga; rojen, ne ustvarjen, enega bistva z Očetom in je po njem vse ustvarjeno; ki je zaradi nas ljudi in zaradi našega zveličanja prišel iz nebes.

In se je utelesil po Svetem Duhu iz Marije Device in postal človek. Bil je tudi križan za nas pod Poncijem Pilatom, je trpel in bil v grob položen. In tretji dan je od mrtvih vstal, po pričevanju Pisma. In je šel v nebesa, sedi na desnici Očetovi. In bo spet prišel v slavi sodit žive in mrtve; in njegovemu kraljestvu ne bo konca.

In v Svetega Duha, Gospoda, ki oživlja; ki izhaja iz Očeta in Sina; ki ga z Očetom in Sinom molimo in slavimo; ki je govoril po prerokih. In eno, sveto, katoliško in apostolsko Cerkev. Priznavam en krst v odpuščanje grehov. In pričakujem vstajenja mrtvih in življenja v prihodnjem veku. Amen.

VELIKI RAZKOL

- Razpad Rima in vzpon Bizanca (l. 395)
- Vprašanje papeževega prvenstva (centralizacija v Rimu)
- 5 patriarhov
- Rimski patriarh (papež) jim je želel biti nadrejen
- primus inter pares
- Vprašanje ali Sveti duh izhaja iz Očeta ali tudi Sina?
- Dodatek Filioqua k Nicejski veroizpovedi
- Filioque = “in Sina”

SHIZMA LETA 1054

- Poslanci papeža Leona IX vs patriarh Mihael I
- Papež sicer umrl pred vzajemnim izobčenjem
- Razkol na rimskokatoliški in pravoslavni del, latinščina vs grščina
- Rimskokatoliški del se je odcepil od pravoslavnega
- Pravoslavni predstavlja staro verigo
- Protestantizem - Luteranstvo, Anglikanstvo, Evangeličanstvo...

RAZPLET

- Pravoslavna veriga je ostala praktično neokrnjena
- Rimskokatoliška veriga je doživela številne spremembe in mutacije
- Kdo je prevladal?
- Število vernikov vs. kvaliteta tradicije

Blocksize War

Razkol znotraj bitcoin skupnosti

BREZMADEŽNO SPOČETJE BITCOINA

/

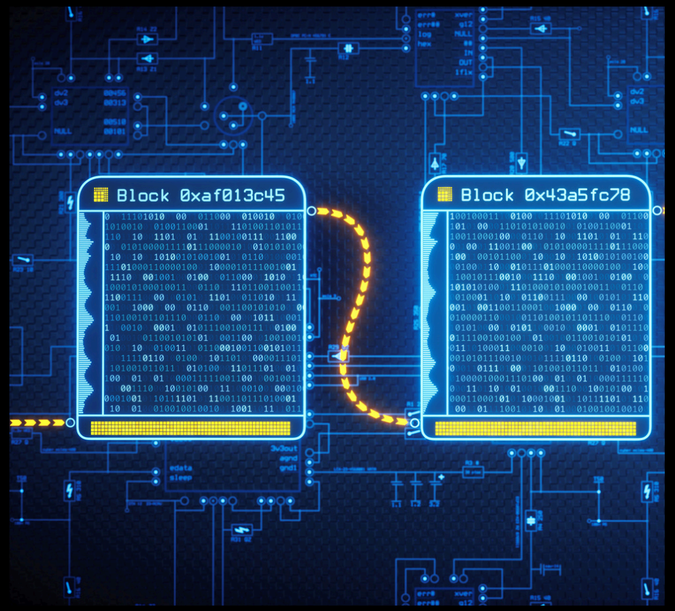
PARUZIJA

Satoshi Nakamoto

- 03.01.2009 je Satoshi ustvaril genesis blok
- Kovancev iz bloka #0 ni mogoče zapraviti
- Satoshi je objavil bitcoin source code 6 dni po genesis bloku, 09.01.2009
- 2. blok je bil prirudarjen šele 7. dan
- Satoshi ob izginotju dostop do domene prepustil Gavinu Andresenu

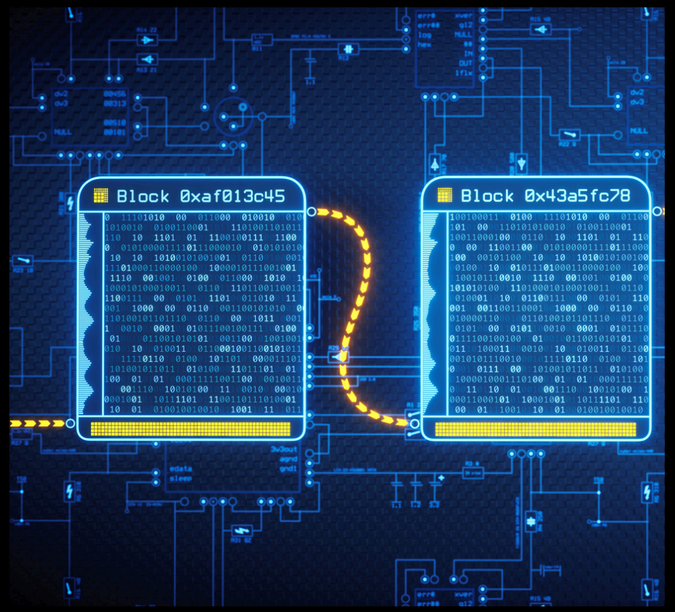
OMEJITEV BLOKA

- Julija 2010 je Satoshi dodal omejitev bločnega prostora na 1MB
- Soft fork utesni pravila omrežja
- Hard Fork sprosti/spremeni pravila in je tako nekompatibilen s staro verzijo
- static const unsigned int MAX_BLOCK_SIZE = 1000000



OMEJITEV BLOKA

- Jeff Garzik je omejitvi nasprotoval
- Satoshi ni pojasnil razloga za omejitev
- V kasnejših komentarjih dopuščal možnost povečanja blocksiza v prihodnosti

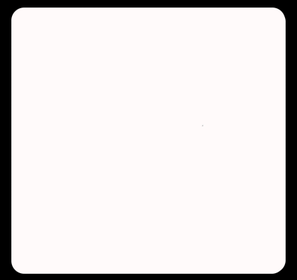


BLOCKSIZE WAR

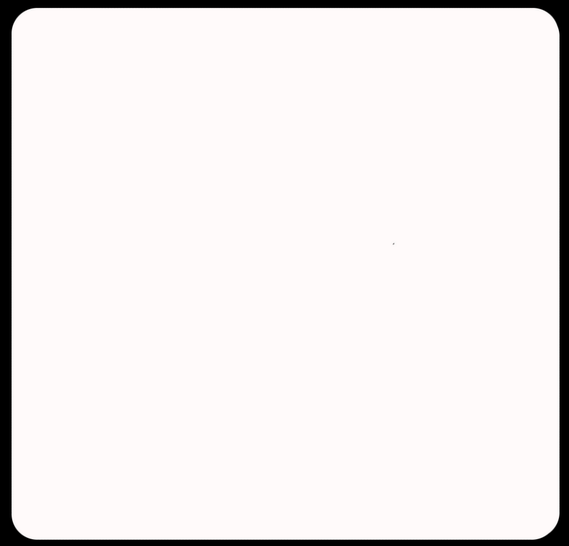
Bitcoin

vs

BitcoinCash



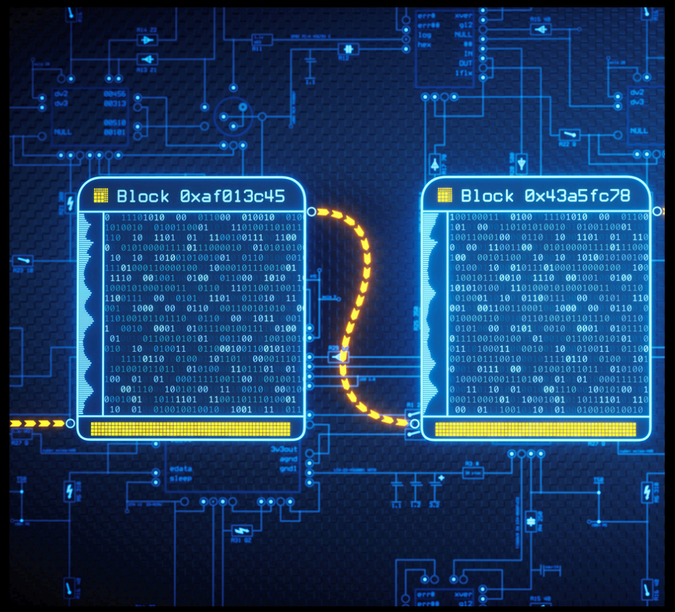
Mali blokerji



Veliki blokerji

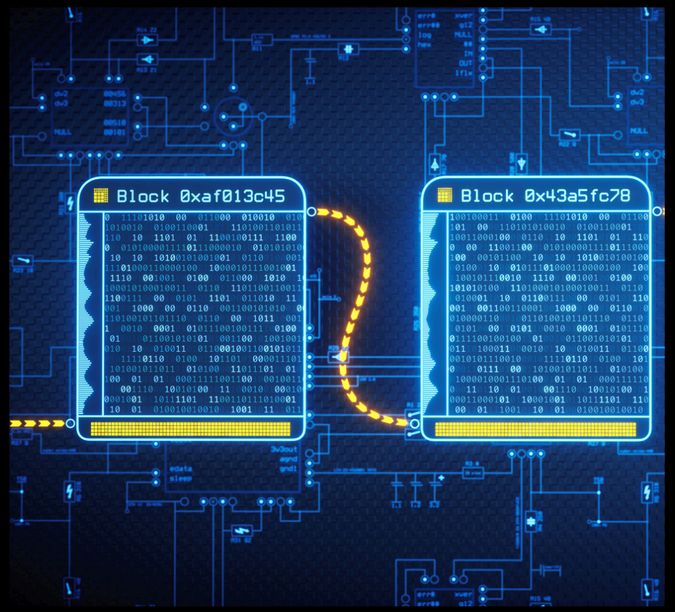
BISTVENA NASPROTOVANJA

- Velikost blokov
- Metodologija implementacije sprememb
- Kdo ima nadzor nad omrežjem
- Časovna preferenca



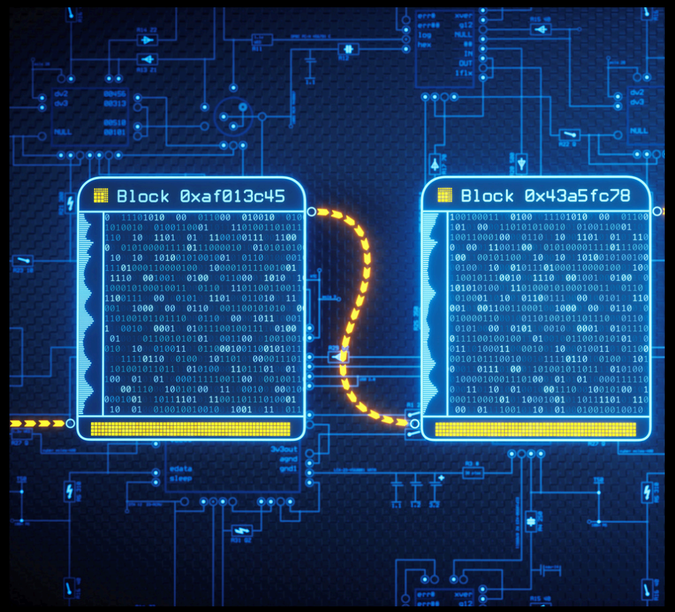
POLITIKA

- Uporabniki VS minerji
- Decentralizacija
- Konsenz ali sledenje vodjam?
- Konkurenca fiat sistemu ali plačilnim posrednikom?



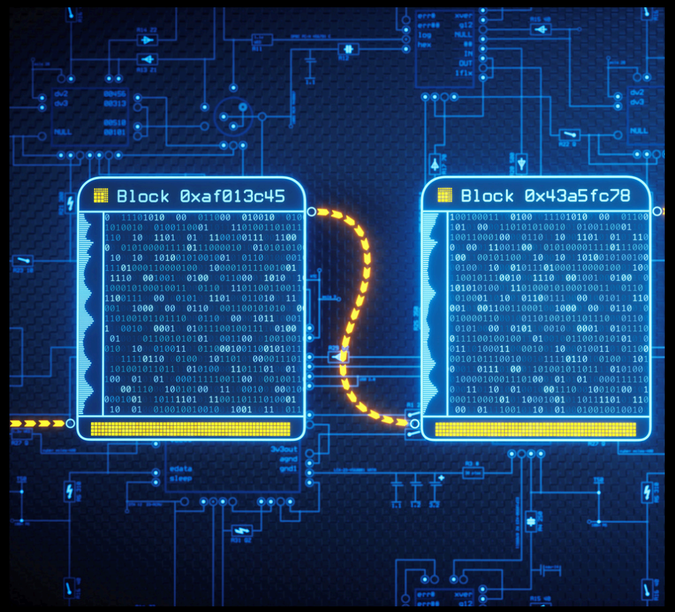
EKONOMIJA

- Monetarni sistem ali plačilni sistem
- Poravnave večjih zneskov ali mikrotransakcije
- Provizijski trg



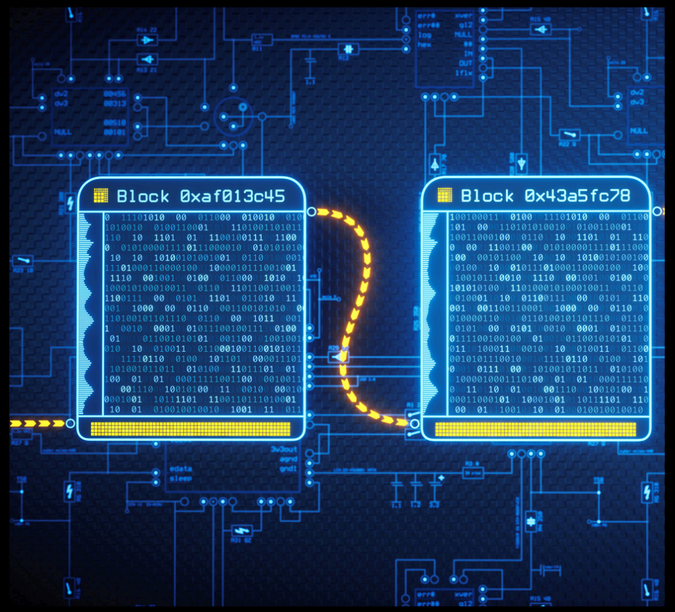
TEHNOLOGIJA

- Razpon/bandwidth
- Transakcijski volumen
- Hardfork vs softfork
- Skaliranje na osnovnem/višjih nivoju/ih
- Varnost ali uporabniška izkušnja



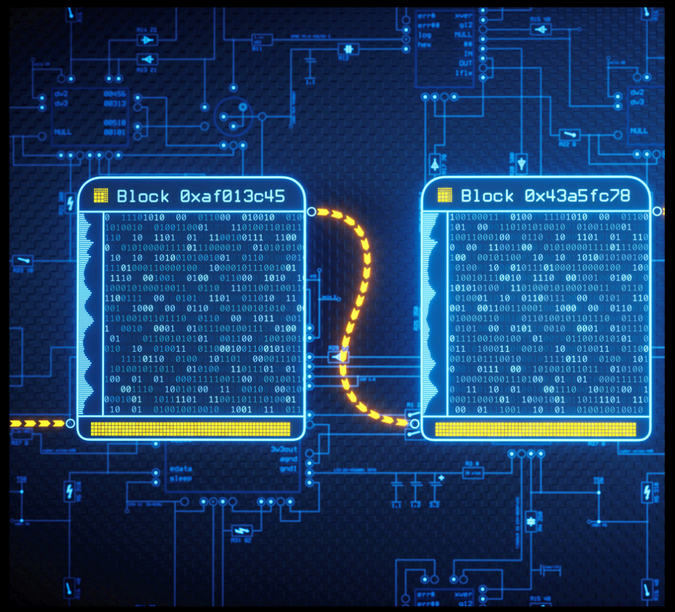
IDEOLOGIJA

- Satoshijeva vizija
- Osifikacija vs posodobitve



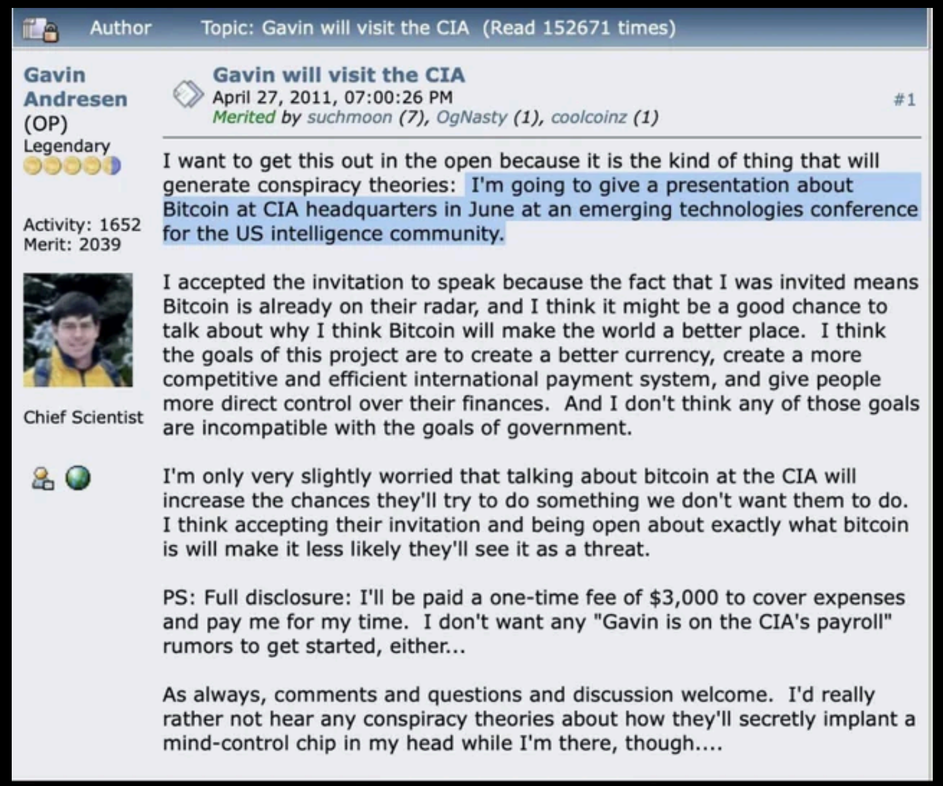
ZAČETEK

- 2015, Gavin Andresen & Mike Hearn
- Bitcoin XT (BIP101)
- Eksponentno rastoči blocksize do 8GB!!
- Gavin verjel, da je vodja skupnosti
- Pismo podpore velikih podjetij



GAVIN ANDRESEN

- Zgodnji Bitcoiner
- Satoshijev zaupnik
- Spoštovan
- Obiskal sedež CIE
- Imel dostop do Sourceforge repozitorija bitcoinove kode
- Soustanovil Bitcoin Foundation
- Prvi plačan bitcoin razvijalec
- Tretirali so ga za “vodjo in obraz” bitcoina



Author | Topic: Gavin will visit the CIA (Read 152671 times)

Gavin Andresen
(OP)
Legendary

Activity: 1652
Merit: 2039

Chief Scientist

Gavin will visit the CIA
April 27, 2011, 07:00:26 PM #1
Merited by suchmoon (7), OgNasty (1), coolcoinz (1)

I want to get this out in the open because it is the kind of thing that will generate conspiracy theories: I'm going to give a presentation about Bitcoin at CIA headquarters in June at an emerging technologies conference for the US intelligence community.

I accepted the invitation to speak because the fact that I was invited means Bitcoin is already on their radar, and I think it might be a good chance to talk about why I think Bitcoin will make the world a better place. I think the goals of this project are to create a better currency, create a more competitive and efficient international payment system, and give people more direct control over their finances. And I don't think any of those goals are incompatible with the goals of government.

I'm only very slightly worried that talking about bitcoin at the CIA will increase the chances they'll try to do something we don't want them to do. I think accepting their invitation and being open about exactly what bitcoin is will make it less likely they'll see it as a threat.

PS: Full disclosure: I'll be paid a one-time fee of $3,000 to cover expenses and pay me for my time. I don't want any "Gavin is on the CIA's payroll" rumors to get started, either...

As always, comments and questions and discussion welcome. I'd really rather not hear any conspiracy theories about how they'll secretly implant a mind-control chip in my head while I'm there, though....

bitcoin history

SATOSHIJEVA PARUZIJA

- Skrinostni e-mail iz l. 2015
- Satoshi@vistomail.com
- Branil vidik malih blokerjev
- Hackan mail?

[bitcoin-dev] Bitcoin XT Fork

Satoshi Nakamoto satoshi at vistomail.com
Sat Aug 15 17:43:54 UTC 2015

- Previous message: [bitcoin-dev] Bitcoin XT 0.11A
- Next message: [bitcoin-dev] Bitcoin XT Fork
- **Messages sorted by:** [date] [thread] [subject] [author]

I have been following the recent block size debates through the mailing list. I had hoped the debate would resolve and that a fork proposal would achieve widespread consensus. However with the formal release of Bitcoin XT 0.11A, this looks unlikely to happen, and so I am forced to share my concerns about this very dangerous fork.

The developers of this pretender-Bitcoin claim to be following my original vision, but nothing could be further from the truth. When I designed Bitcoin, I designed it in such a way as to make future modifications to the consensus rules difficult without near unanimous agreement. Bitcoin was designed to be protected from the influence of charismatic leaders, even if their name is Gavin Andresen, Barack Obama, or Satoshi Nakamoto. Nearly everyone has to agree on a change, and they have to do it without being forced or pressured into it. By doing a fork in this way, these developers are violating the "original vision" they claim to honour.

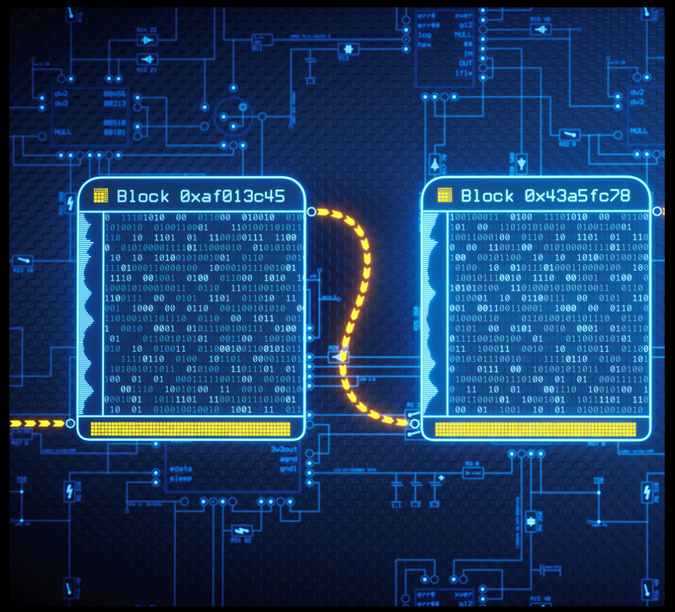
They use my old writings to make claims about what Bitcoin was supposed to be. However I acknowledge that a lot has changed since that time, and new knowledge has been gained that contradicts some of my early opinions. For example I didn't anticipate pooled mining and its effects on the security of the network. Making Bitcoin a competitive monetary system while also preserving its security properties is not a trivial problem, and we should take more time to come up with a robust solution. I suspect we need a better incentive for users to run nodes instead of relying solely on altruism.

If two developers can fork Bitcoin and succeed in redefining what "Bitcoin" is, in the face of widespread technical criticism and through the use of populist tactics, then I will have no choice but to declare Bitcoin a failed project. Bitcoin was meant to be both technically and socially robust. This present situation has been very disappointing to watch unfold.

Satoshi Nakamoto

CENTRALIZIRANOST

- Odločitev na strani borz in rudarjev?
- Mike ima zadnjo besedo pri XT

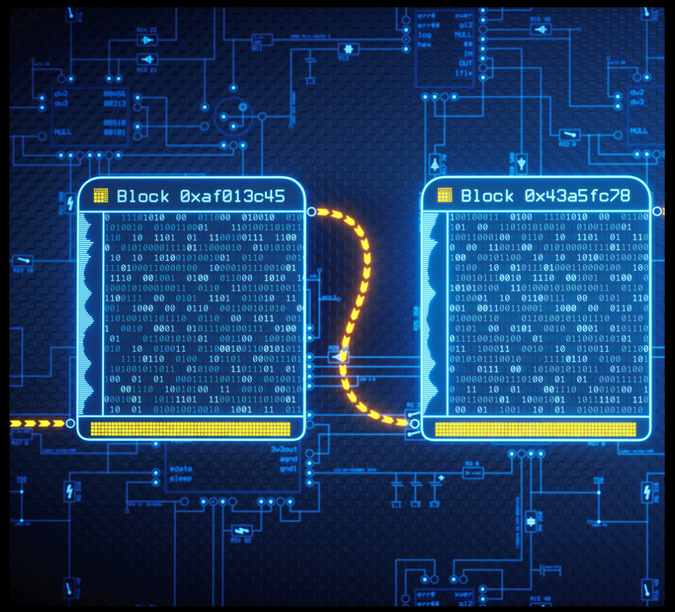


SCALING I - MONTREAL

- December 2015
- Prva konferenca na temo povečanja blokov
- Gregory Maxwell vs Gavin Andresen
- Gregory soustanovil Blockstream l. 2014
- Konflikt interesov?
- Prisotnost Rogerja Vera, Bitcoin Jezusa

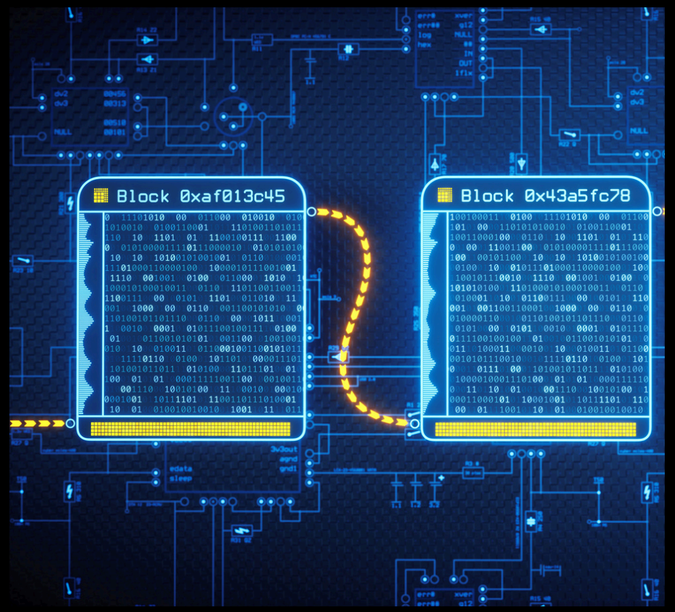
ROGER VER

- Glasen zagovornik bitcoina
- Podpiral adopcijo trgovcev
- Videl bitcoin kot superiorno plačilno sredstvo
- Lastnik subreddita r/btc
- Miril uporabnike Mt. Goxa o solvenčnosti borze
- Postal lastnik bitcoin.com domene



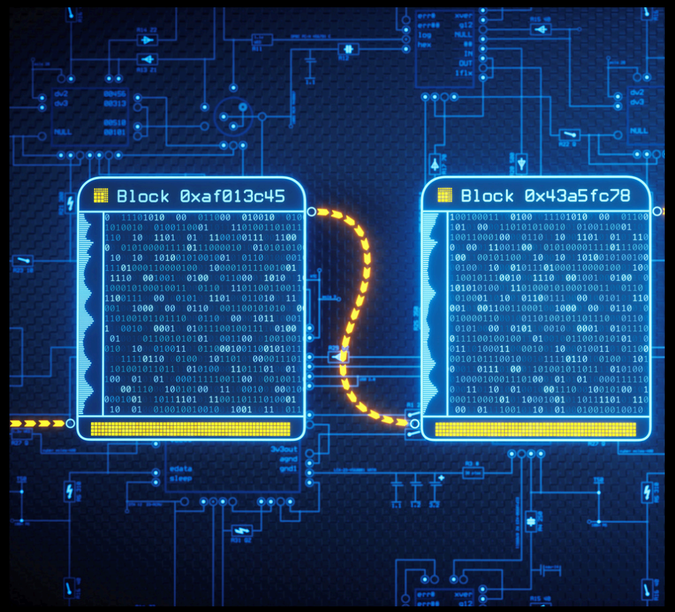
SEGWIT

- Najpomembnejši preboj v konfliktu
- LukeDashJr iznašel trik za povečanje prostora brez potrebe po odcepu verige (hardforku)
- Hkrati rešil problem spreminjanja transakcij (transaction malleability)
- Omogočil Lightning in mikroplačila
- Rešil problem nelinearnega skaliranja sighash operacij
- Izjemno tehnično kompliciran



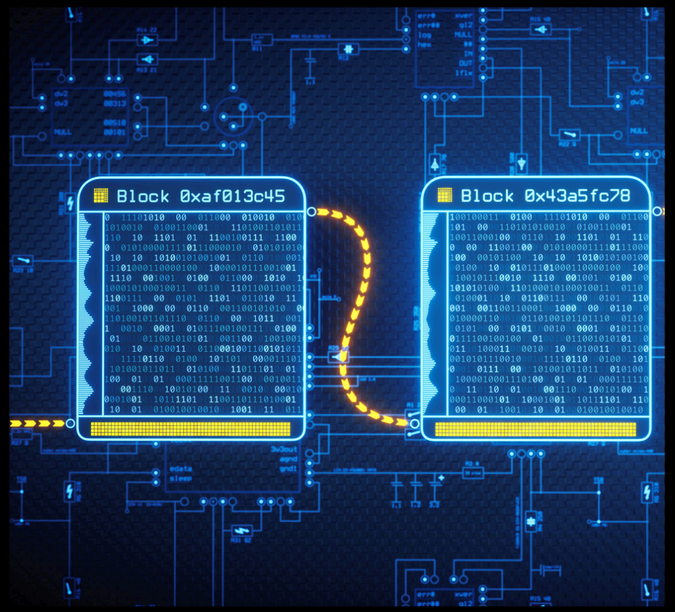
SEGWIT

- Zahtevnejši način implementacije
- Utesnitev pravil protokola (softfork)
- Zahteva 95% konsenz rudarjev
- Standardna metodologija implementacije
- Predlagan konec l. 2015, izdan na Bitcoin Core šele leto po tem



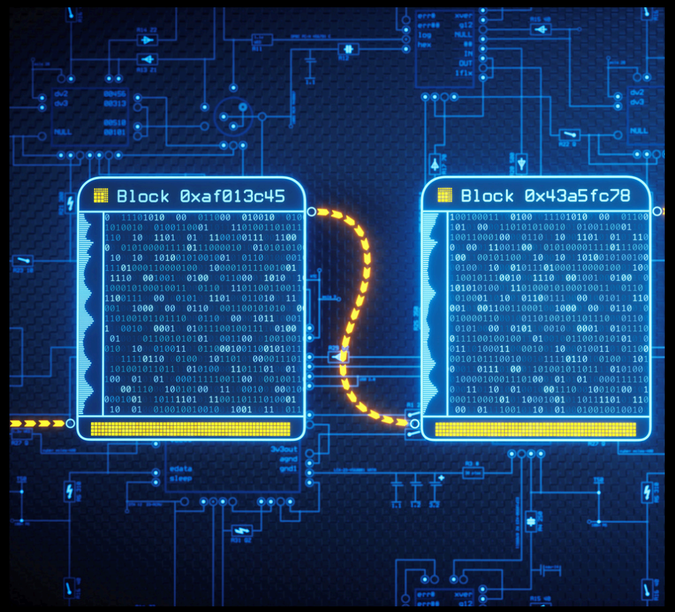
LIGHTNING

- Idejo je predlagal že Satoshi
- Lightning White Paper l. 2015
- Implementacija šele l. 2018
- Zasebnost
- Hitrost
- Konkurent Visi & Mastercardu



BITCOIN CLASSIC

- spodrsljaj Bitcoin XT
- 10.02.2016 Bitcoin Classic
- Veliki blockerji potrebovali novega paradnega konja
- Gavin Andresen vodilni programer
- Garzik se pridruži
- Preprost skok na 2MB bloke
- Brez wipeout protectiona

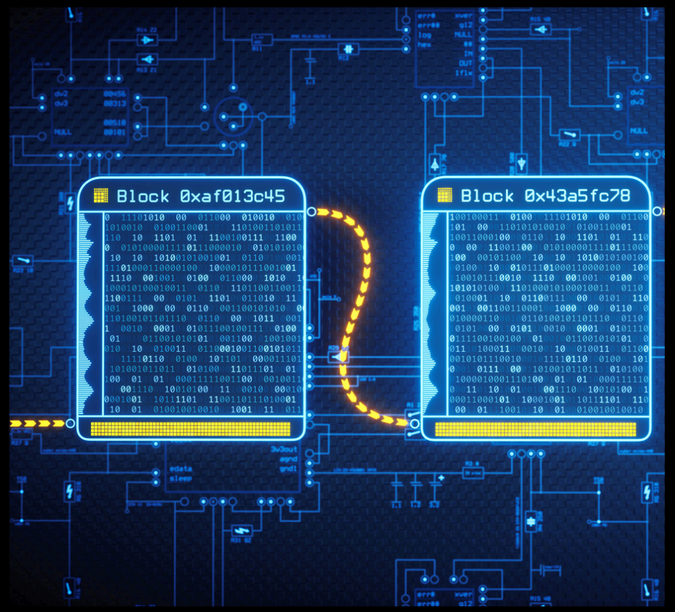


SCALING II HONG KONG

- Debata na temo skaliranja
- Mali blokerji želeli prepričati rudarje
- Jihan Wu & BitMain
- Spor med Core-om in rudarji

GAVIN OBJAVI BLOG

- 02.05.2016
- Verjame, da je Craig Wright Satoshi
- Požre ogromno kritike s strani bitcoinerjev
- Izgubi commit access do Bitcoin Core repozitorija
- Craig Wright objavi dvoumno objavo



CRAIG WRIGHT

- Narcistični spletkar
- Trdil, da je Satoshi
- Tožil bitcoin skupnost
- Želel avtorsko zaščititi White Paper
- Veliki bloker
- BSV

ETHEREUM

- Nastal l. 2015
- Privabil številne velike blokerje
- DAO, $150mio
- DAO hack l. 2016 -> DAO wars

DAO WARS

- Hardfork, sprva ni prišlo do razcepa
- Wipeout protection
- Razcep verige, delitev na ETH in ETC
- Ethereumov razcep prestrašil Bitcoin rudarje
- Velik korak za male blokerje
- Eth rešil Bitcoin?

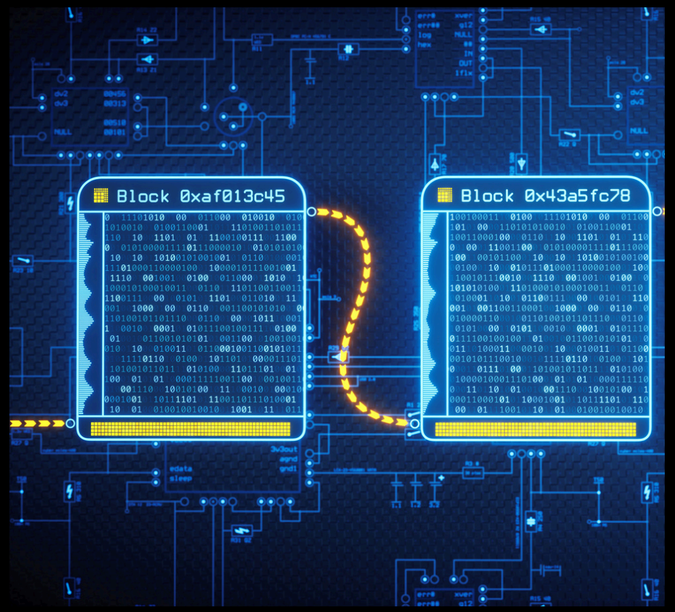
SCALING III MILANO

- 08.10.2016
- Dogodek dominirali mali blokerji
- Očitnost preobrata v vojni
- Pogovori na temo SegWita
- Prisotnost Vera in podpornikov

  Bitcoin Unlimited

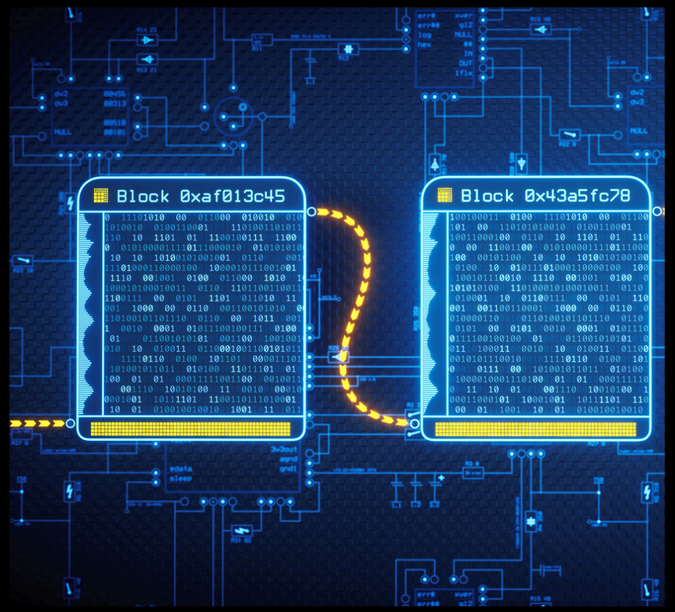
BITCOIN UNLIMITED

- ogromno napak
- tehnične spremembe
- podpora industrije
- velika napaka



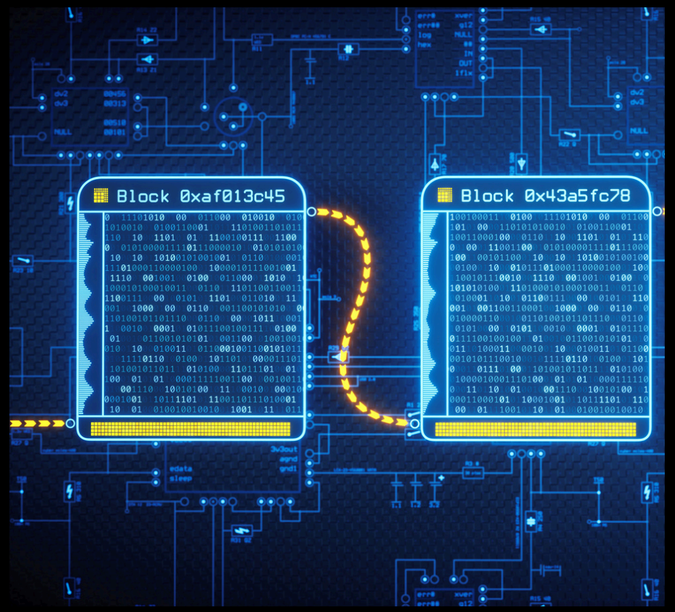
SEGWIT CONT. &. 2017

- ASICBoost
- BitMain
- Lažnivi akterji?
- Integracija na LTC
- Borze zavrnejo Bitcoin Unlimited



NEW YORK AGREEMENT

- Pizza Day 2017
- Aktivirati SegWit z 80% rudarske podpore
- Aktivirati 2MB bloke po 6. mesecih
- Vzajemni dogovor med obema poloma
- PR stunt?
- Minerji želeli prikazati, da imajo nadzor



BITCOIN CASH

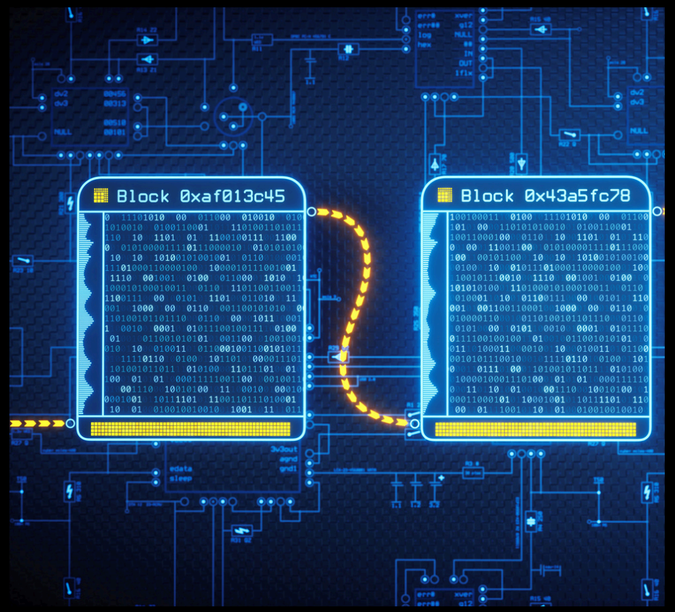
- Na konferenci velikih blokerjev naznanjen klient Bitcoin ABC
- Poimenovan BCC = Bitcoin Cash
- Brez SegWita, omogoča ASICBoost
- Drugačen difficulty adjustment
- nekompatibilen z Bitcoinom
- Zadnji skupni blok #478.559

BITCOIN CASH CONT.

- 8MB bloki
- Najvišja vrednost, ki jo je dosegel je 8.500$
- Največ 48% vrednosti BTC
- Danes nekje 1% vrednosti BTC
- Volumen transakcij nižji od volumna na BTC kljub nizkim feejem
- Doživel več nadaljnjih odcepov (BSV...)

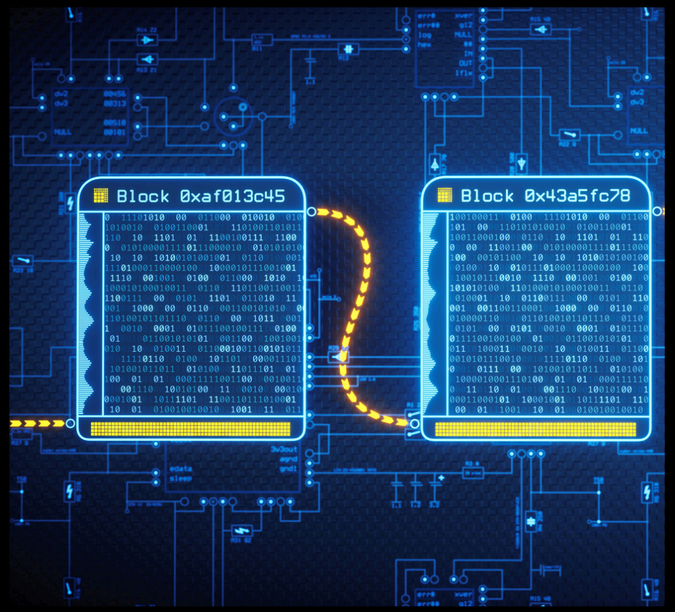
SCALING IV STANFORD

- 04.11.2017
- Brez govora o blocksizu
- Drugi del NYA-SegWit2x
- Implementacija 2MB hardforka na Bitcoinu
- 08.11.2017 konec vojne po 816 dneh



ZAKLJUČEK

- Prevlada malih blokerjev
- Bitcoin nadzirajo uporabniki
- Satoshijev protokol ostaja nespremenjen
- SegWit ima višji volumen od celotnega BCH
- Spremembe morajo doseči konsenz brez prisile
- Bitcoin je dolgoročni monetarni projekt, ki ogroža obstoj fiatnega sistema
- Skalira v slojih



bitcoinshop

bitcoinslovenia

bitcoinknjiznica