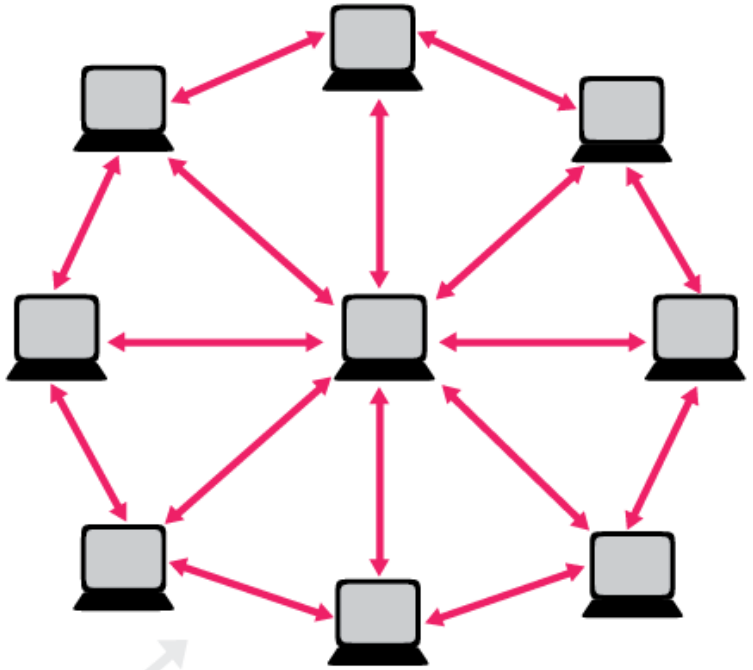
BLOCKCHAIN

Nastja Cepak
Inštitut Andrej Marušič, UP
CREA plus d.o.o.

Blockchain:

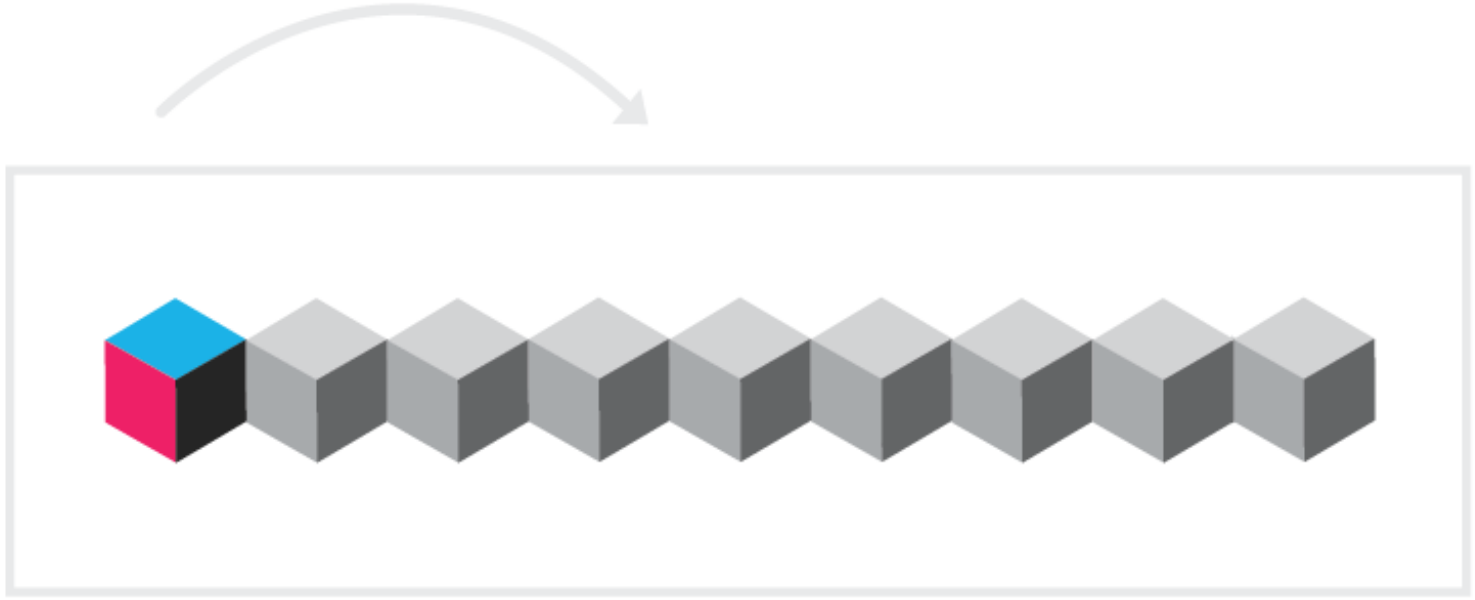
Porazdeljena programska baza, ki nepokvarljivo hrani naraščajočo listo transakcij.

Nekdo zahteva **transakcijo**.



Transakcija je predana P2P **omrežju**, ki ga sestavljajo računalniki.

Omrežje **potrdi** transakcijo in status uporabnikov s poznanim algoritmom.



Potrjena transakcija je skupaj z drugimi transakcijami združena v **blok** podatkov.

Novi blok je dodan že obstoječi verigi blokov, **blockchainu**, trajno in nespremeljivo.

Transakcija je **zaključena**.

Transakcija

Transakcija

Transakcija

Transakcija

Transakcija

Transakcija

Kdaj

prve ideje?

prvi blockchain?

Kdo?

Kaj/Kateri?

Kdaj

prve ideje? 80. leta

prvi blockchain?

Kdo?

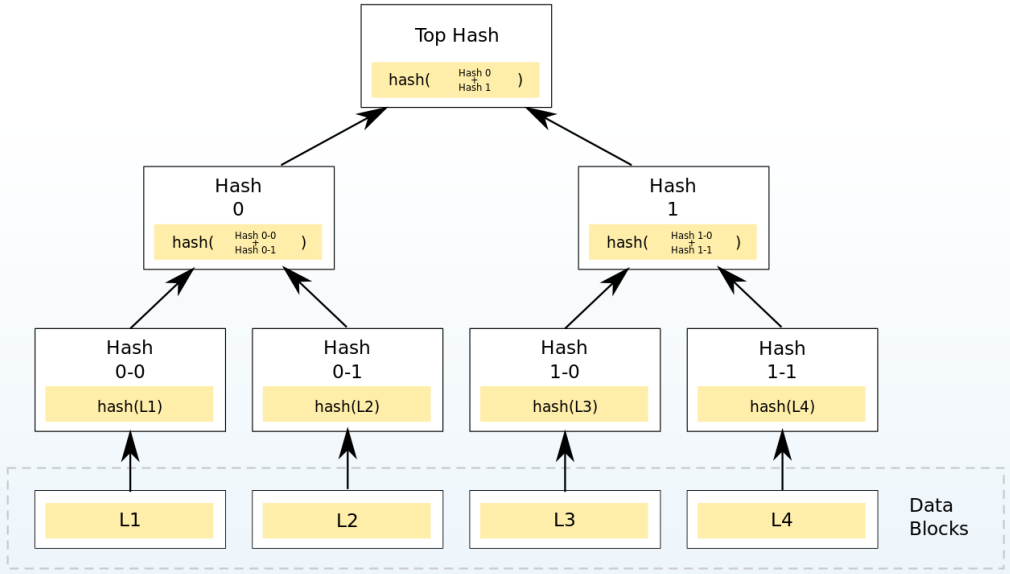
Kaj/Kateri?

Plačila brez centralne avtoritete

Kako varno, necetralizirano **POTRJEVATI TRANSAKCIJE**: Proof of work

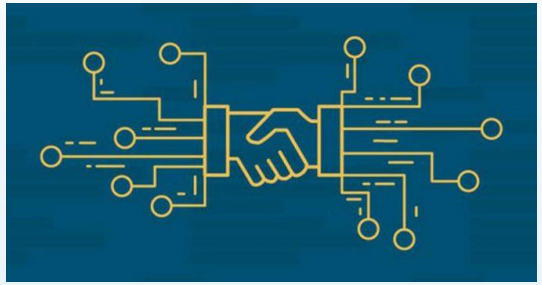
KDAJ je bil dokument narejen: timestamping

Kako več dokumentov združiti v **EN BLOK**: Merklova drevesa



Prvi Cypherpunk manifesto

Predstavljena ideja **PAMETNIH POGODB**



Kdaj

prve ideje? 80. leta

prvi blockchain?

Kdo?

Kaj/Kateri?

Kdaj

prve ideje? 80. leta

prvi blockchain? 2008/2009

Kdo?

Kaj/Kateri?

Kdaj

prve ideje? 80. leta

prvi blockchain? 2008/2009

Kdo? Satoshi Nakamoto

Kaj/Kateri?

Kdaj

prve ideje? 80. leta

prvi blockchain? 2008/2009

Kdo? Satoshi Nakamoto

Kaj/Kateri?

Kriptovalute

Kriptovalute

Kriptovaluta je blockchain.
Nima fizične oblike.

```
00000000   01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000010   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000020   00 00 00 00 3B A3 ED FD  7A 7B 12 B2 7A C7 2C 3E   ....;£íýz{.²zÇ,>
00000030   67 76 8F 61 7F C8 1B C3  88 8A 51 32 3A 9F B8 AA   gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040   4B 1E 5E 4A 29 AB 5F 49  FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iÿÿ...¬+|
00000050   01 01 00 00 00 01 00 00  00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 FF FF  FF FF 4D 04 FF FF 00 1D   ......ÿÿÿÿM.ÿÿ..
00000080   01 04 45 54 68 65 20 54  69 6D 65 73 20 30 33 2F   ..EThe Times 03/
00000090   4A 61 6E 2F 32 30 30 39  20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
000000A0   6C 6F 72 20 6F 6E 20 62  72 69 6E 6B 20 6F 66 20   lor on brink of
000000B0   73 65 63 6F 6E 64 20 62  61 69 6C 6F 75 74 20 66   second bailout f
000000C0   6F 72 20 62 61 6E 6B 73  FF FF FF FF 01 00 F2 05   or banksÿÿÿÿ..ò.
000000D0   2A 01 00 00 00 43 41 04  67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
000000E0   19 67 F1 A6 71 30 B7 10  5C D6 A8 28 E0 39 09 A6   .gñ¦q0·.\Ö¨(à9.¦
000000F0   79 62 E0 EA 1F 61 DE B6  49 F6 BC 3F 4C EF 38 C4   ybàê.aÞ¶Iö¼?Lï8Ä
00000100   F3 55 04 E5 1E C1 12 DE  5C 38 4D F7 BA 0B 8D 57   óU.å.Á.Þ\8M÷°..W
00000110   8A 4C 70 2B 6B F1 1D 5F  AC 00 00 00 00            ŠLp+kñ._¬....
```

Kriptovalute

Kriptovaluta je blockchain.
Nima fizične oblike.

Zaloge ne določa
centralna banka.

Kriptovalute

Kriptovaluta je blockchain.
Nima fizične oblike.

Zaloge ne določa
centralna banka.

Omrežje je povsem
decentralizirano.

Potrjevanje transakcij

Omrežje **potrdi** transakcijo in status uporabnikov s poznanim algoritmom.

- Potrjevanje poteka z uproabo **algoritmov konsenza**.
- Eden najbolje poznanih takšnih algoritmov je **Proof of Work** (PoW), ki ga med drugim uporablja Bitcoin.
- Obstajajo tudi številni drugi: Proof of Stake, Proof of Burn, Proof of Authority, Proof of Capacity,...

Proof of Work

podatki prejšnjega bloka

transakcija

iskana neznana vrednost

hash funkcija/
razpršilna funkcija

00…0xy…z

najti 

=

potrditi transakcijo

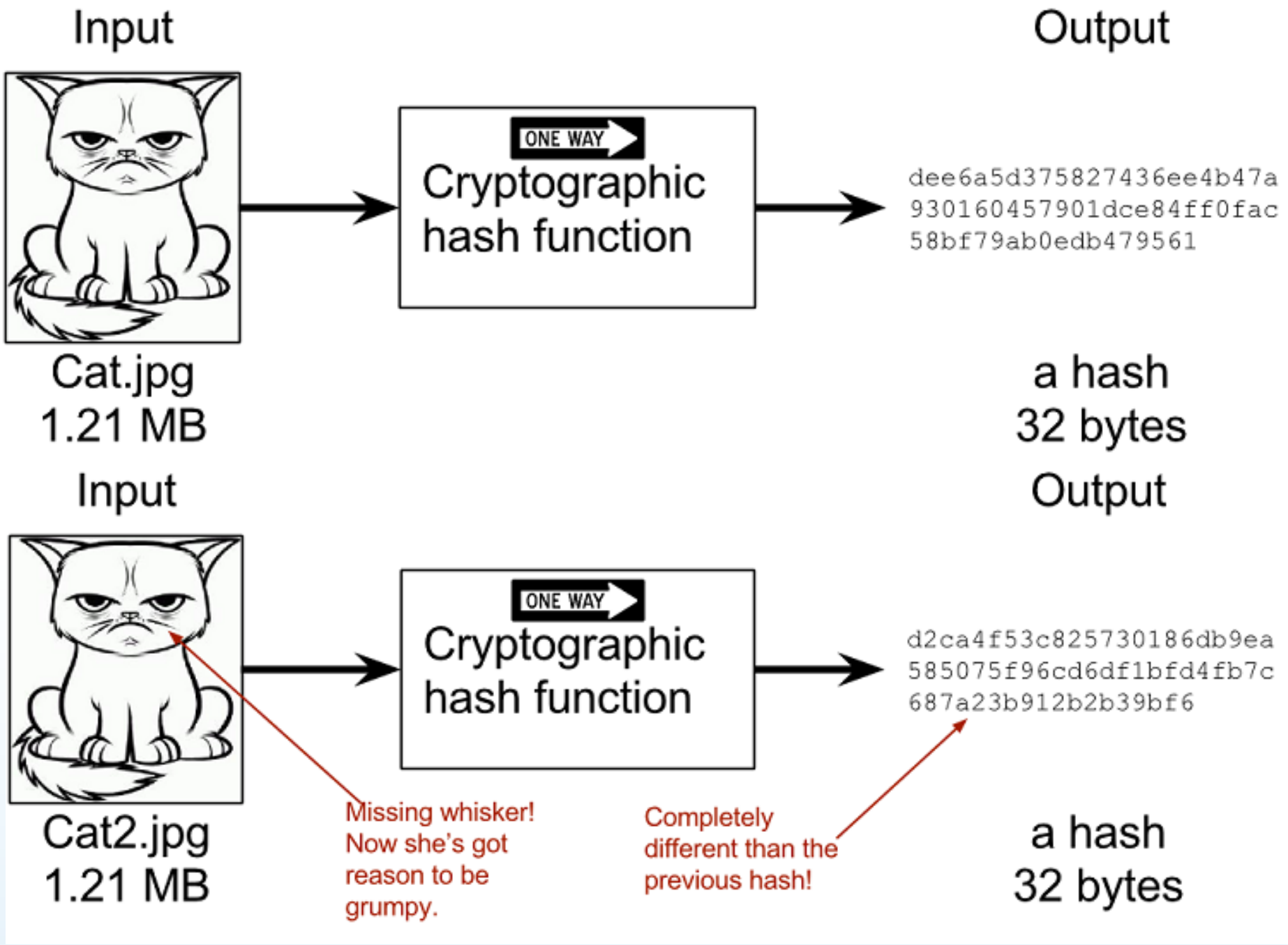
Input

Cat.jpg
1.21 MB

Output

```
dee6a5d375827436ee4b47a
930160457901dce84ff0fac
58bf79ab0edb479561
```

a hash
32 bytes


Input
Output
ONE WAY
Cryptographic hash function
dee6a5d375827436ee4b47a
930160457901dce84ff0fac
58bf79ab0edb479561
Cat.jpg
1.21 MB
a hash
32 bytes
Input
Output
ONE WAY
Cryptographic hash function
d2ca4f53c825730186db9ea
585075f96cd6df1bfd4fb7c
687a23b912b2b39bf6
Missing whisker! Now she's got reason to be grumpy.
Completely different than the previous hash!
Cat2.jpg
1.21 MB
a hash
32 bytes

Proof of Work

podatki prejšnjega bloka

transakcija

iskana neznana vrednost

hash funkcija/
razpršilna funkcija

00…0xy…z

najti 

=

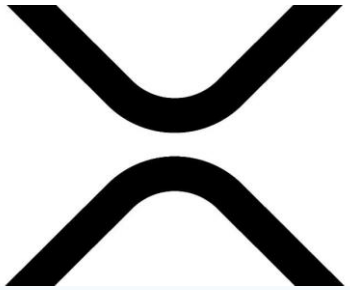
potrditi transakcijo

Rudarjenje

Altcoin

Kriptovaluta, ki ni Bitcoin.

Ethereum



Ripple

Bitcoin Cash

Litecoin

Monero

Trumpcoin


Kriptografski
Kako zagotavljati varnost?
Programerski
Kako učinkovito implementirati?
4 glavni aspekti
Ekonomski
Kako blockchain dobičkonosno uporabiti?
Družbeni
V katero smer gre dolgoročni razvoj in kakšen bo njegov vpliv?

Kriptografija

Kriptografija

Avtentikacija uporabnika

Potrjevanje transakcij

Kriptografija

Avtentikacija uporabnika

- Asimetrična kriptografija
  javni in zasebni ključi!
- Eliptične krivulje
- Pri ključu enake dolžine je ECC več kot 10x varnejša od RSA

Potrjevanje transakcij

Kriptografija

Avtentikacija uporabnika

- Asimetrična kriptografija
  privatni in zasebni ključi!
- Eliptične krivulje
- Pri ključu enake dolžine je ECC več kot 10x varnejša od RSA

Potrjevanje transakcij

podatki prejšnjega bloka

transakcija

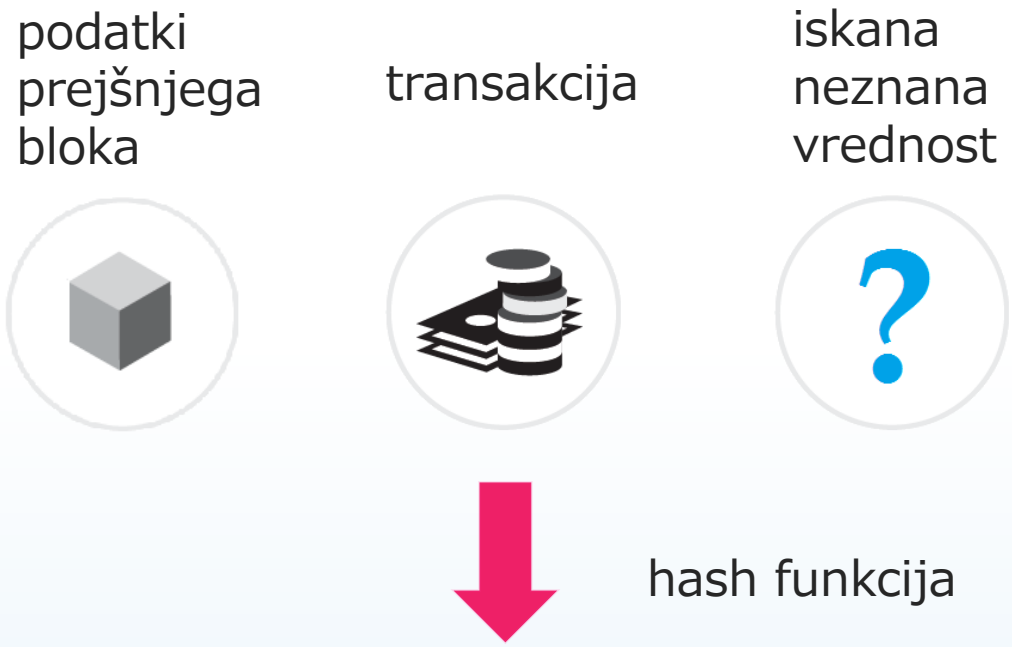
iskana neznana vrednost

Kriptografija

Avtentikacija uporabnika

- Asimetrična kriptografija
  privatni in zasebni ključi!
- Eliptične krivulje
- Pri ključu enake dolžine je ECC več kot 10x varnejša od RSA

Potrjevanje transakcij

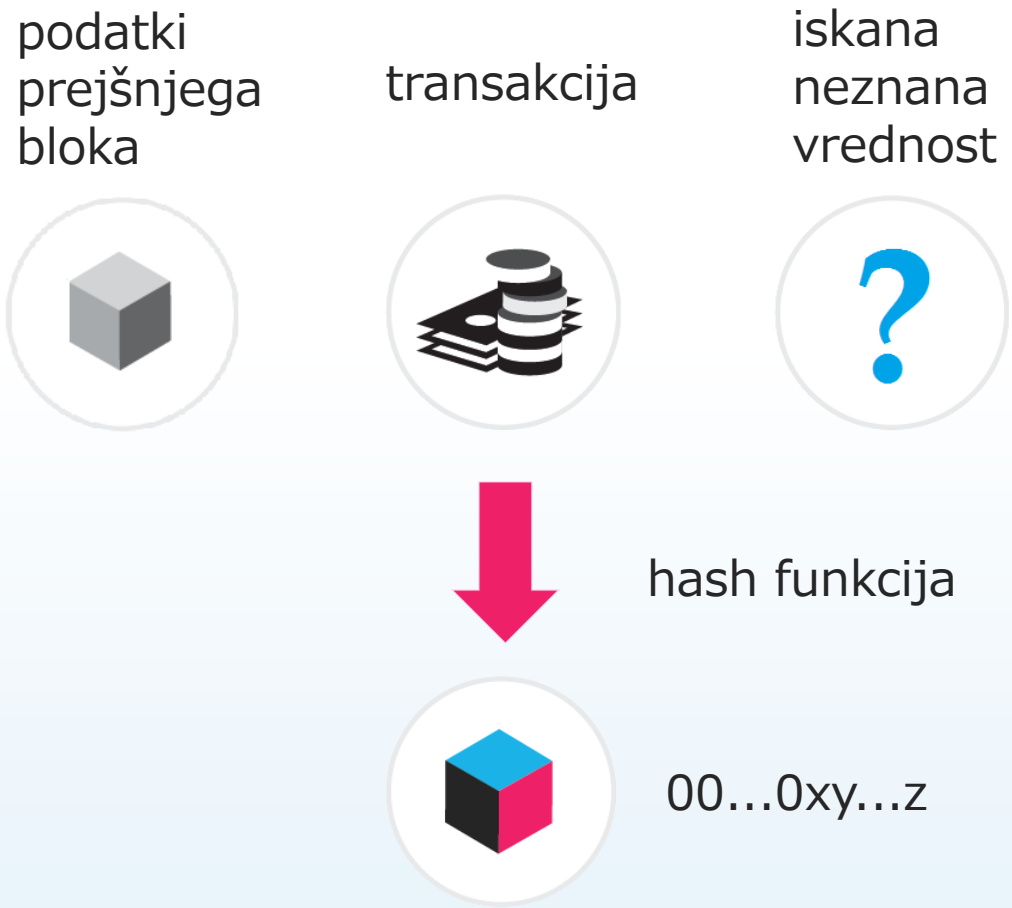


Kriptografija

Avtentikacija uporabnika

- Asimetrična kriptografija
  privatni in zasebni ključi!
- Eliptične krivulje
- Pri ključu enake dolžine je ECC več kot 10x varnejša od RSA

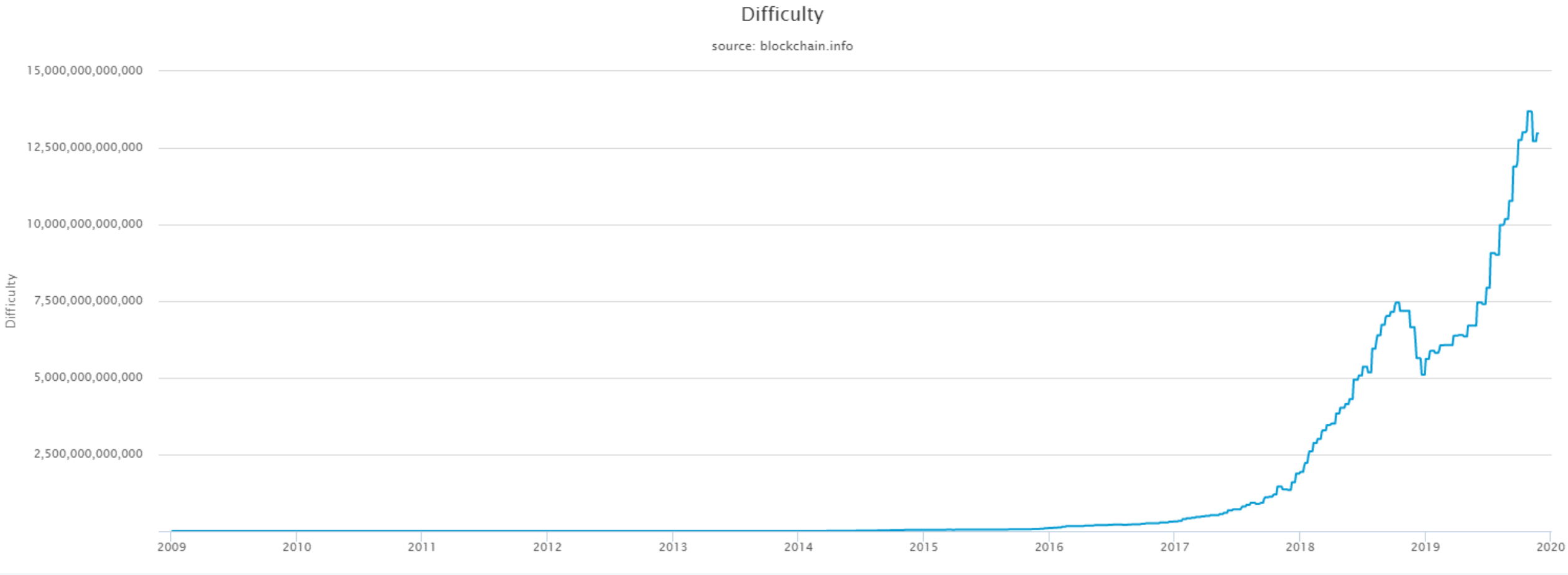
Potrjevanje transakcij



Programiranje

- Določanje težavnosti potrditve transakcije


Difficulty
source: blockchain.info
15,000,000,000,000
12,500,000,000,000
10,000,000,000,000
7,500,000,000,000
5,000,000,000,000
2,500,000,000,000
Difficulty
Jan '18
Mar '18
May '18
Jul '18
Sep '18
Nov '18
Jan '19
Mar '19
May '19
Jul '19
Sep '19
Nov '19


Difficulty
source: blockchain.info
15,000,000,000,000
12,500,000,000,000
10,000,000,000,000
7,500,000,000,000
5,000,000,000,000
2,500,000,000,000
Difficulty
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020

Programiranje

- Določanje težavnosti potrditve transakcije
- Kako posodobiti kodo že obstoječega blockchaina?

Programiranje

- Določanje težavnosti potrditve transakcije
- Kako posodobiti kodo že obstoječega blockchaina?
- Aktualen primer: Bitcoin scalling

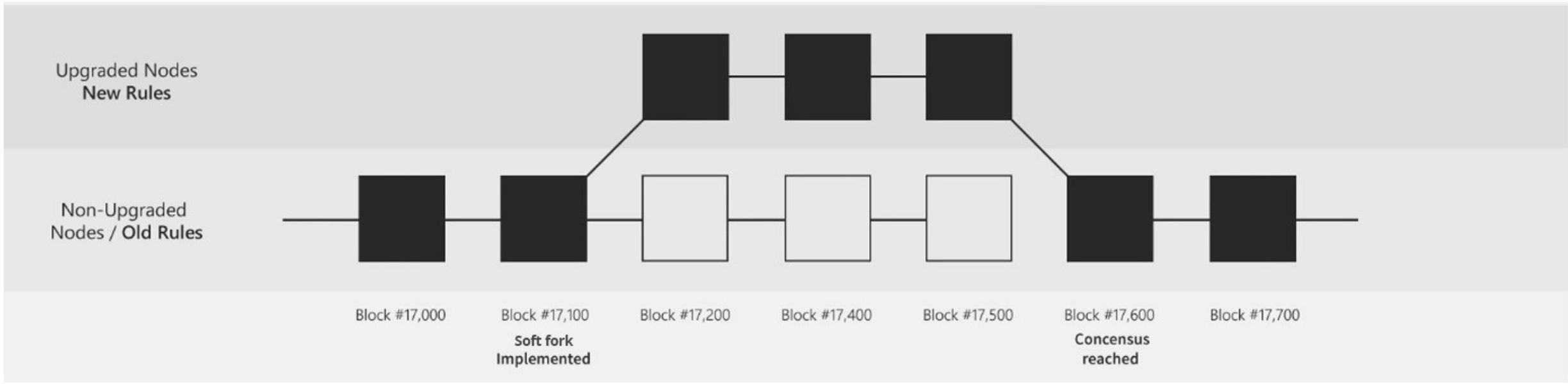
  Bitcoin: ~7 transakcij/s
  Ethereum: ~20 transakcij/s

Soft fork	Hard fork
Strožja pravila	Razširitev pravil
Nazaj kompatibilno	Nekompatibilno
Stari nodes sprejemajo nove bloke	Stari nodes ne sprejemajo novih blokov

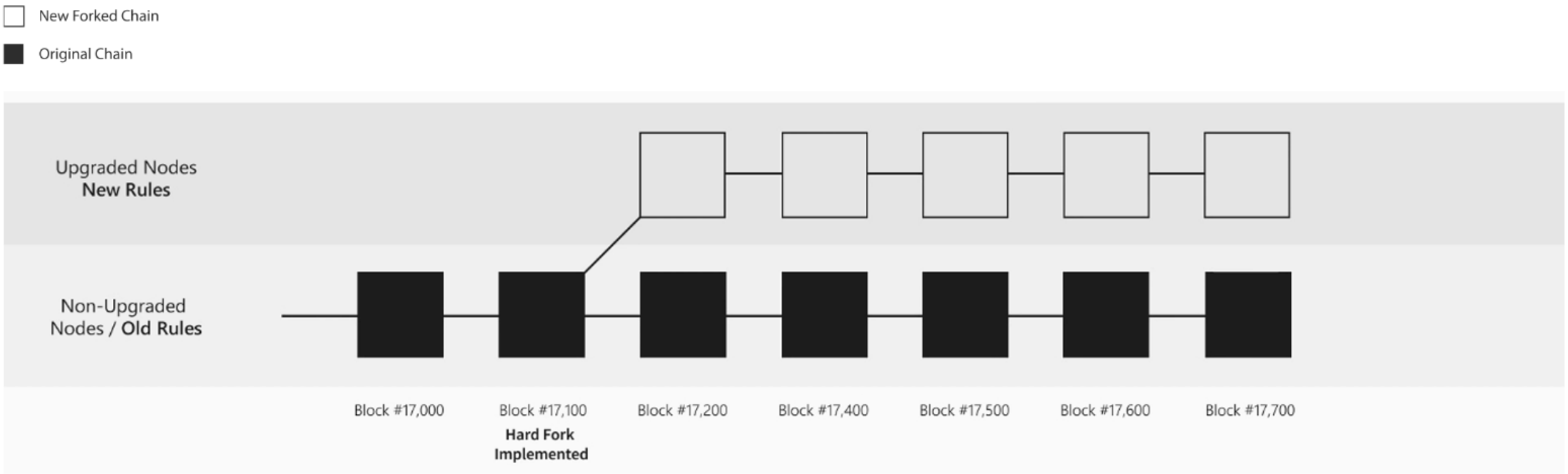
SOFT FORK

Blocks Violating new Rules

Strongest Chain of Blocks



HARD FORK


New Forked Chain
Original Chain
Upgraded Nodes
New Rules
Non-Upgraded
Nodes / Old Rules
Block #17,000
Block #17,100
Hard Fork
Implemented
Block #17,200
Block #17,400
Block #17,500
Block #17,600
Block #17,700

Ekonomija in finance

Ekonomija in finance

Author	Topic: Pizza for bitcoins? (Read 603660 times)

laszlo
Full Member

Activity: 199

Pizza for bitcoins?
May 18, 2010, 12:35:20 AM #1

I'll pay 10,000 bitcoins for a couple of pizzas.. like maybe 2 large ones so I have some left over for the next day. I like having left over pizza to nibble on later. You can make the pizza yourself and bring it to my house or order it for me from a delivery place, but what I'm aiming for is getting food delivered in exchange for bitcoins where I don't have to order or prepare it myself, kind of like ordering a 'breakfast platter' at a hotel or something, they just bring you something to eat and you're happy!

I like things like onions, peppers, sausage, mushrooms, tomatoes, pepperoni, etc.. just standard stuff no weird fish topping or anything like that. I also like regular cheese pizzas which may be cheaper to prepare or otherwise acquire.

If you're interested please let me know and we can work out a deal.

Thanks,
Laszlo

BC: 157fRrqAKrDyGHr1Bx3yDxeMv8Rh45aUet

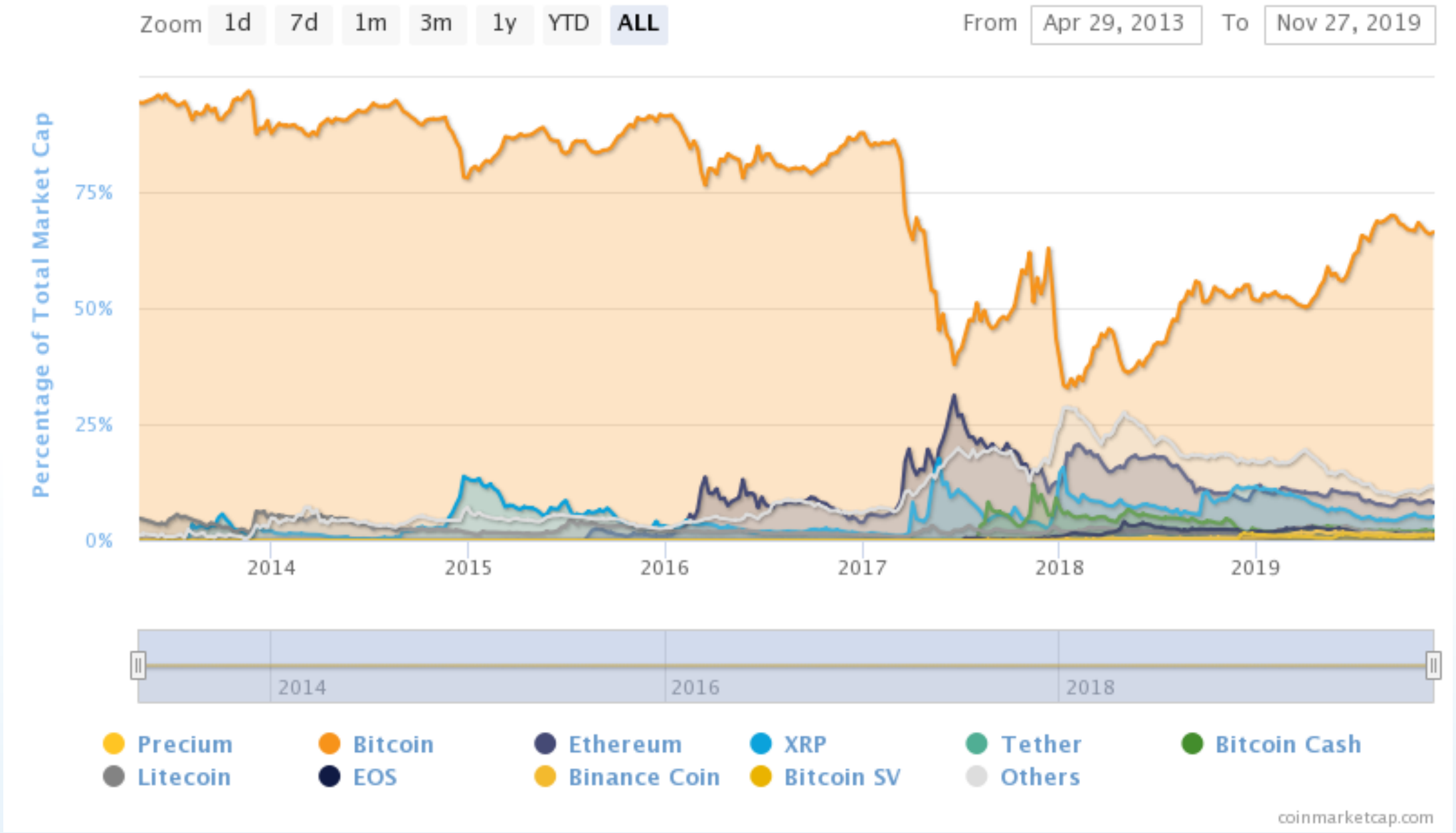

Your Recipe.
Our Ingredients.
Papa's Specialty
Pizza Challenge
Please Recycle


Papa Quality Approved


Your Recipe.
Our Ingredients.
Papa's Specialty
Pizza Challenge
Please Recycle

Ekonomija in finance

Vrednost trga kriptovalut 27.11.2019: $195,301,549,506


Zoom 1d 7d 1m 3m 1y YTD ALL
From Apr 29, 2013 To Nov 27, 2019
Percentage of Total Market Cap
75%
50%
25%
0%
2014
2015
2016
2017
2018
2019
Precium
Bitcoin
Ethereum
XRP
Tether
Bitcoin Cash
Litecoin
EOS
Binance Coin
Bitcoin SV
Others
coinmarketcap.com

- Švicarska banka Bank Vontobel AG je leta 2016 prvič ponudila vlaganje v bitcoin

- Švicarska banka Bank Vontobel AG je leta 2016 prvič ponudila vlaganje v bitcoin

- Ripple – privatna kriptovaluta namenjena bančnim prenosom

Our Clients

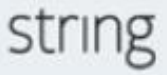

Standard Chartered
UniCredit
Bank of America Merrill Lynch
RBC
Westpac
Santander
BMO
CIBC
UBS
MIZUHO
nab
AXIS BANK
Reise Bank
cross river bank
SHRB
SCB ไทยพาณิชย์
NBAD
SBI Remit
MUFG
Bank of Tokyo-Mitsubishi UFJ
BBVA
SEB
AKBANK
YES BANK
Cambridge
Global Payments
STAR ONE CREDIT UNION
eZforex.com
GLOBALIZING FINANCIAL TECHNOLOGY

- Švicarska banka Bank Vontobel AG je leta 2016 prvič ponudila vlaganje v bitcoin

- Ripple – privatna kriptovaluta namenjena bančnim prenosom

- February 2016 je bila ustanovljena Enterprise Ethereum Alliance https://entethalliance.org/

LAUNCH MEMBERS

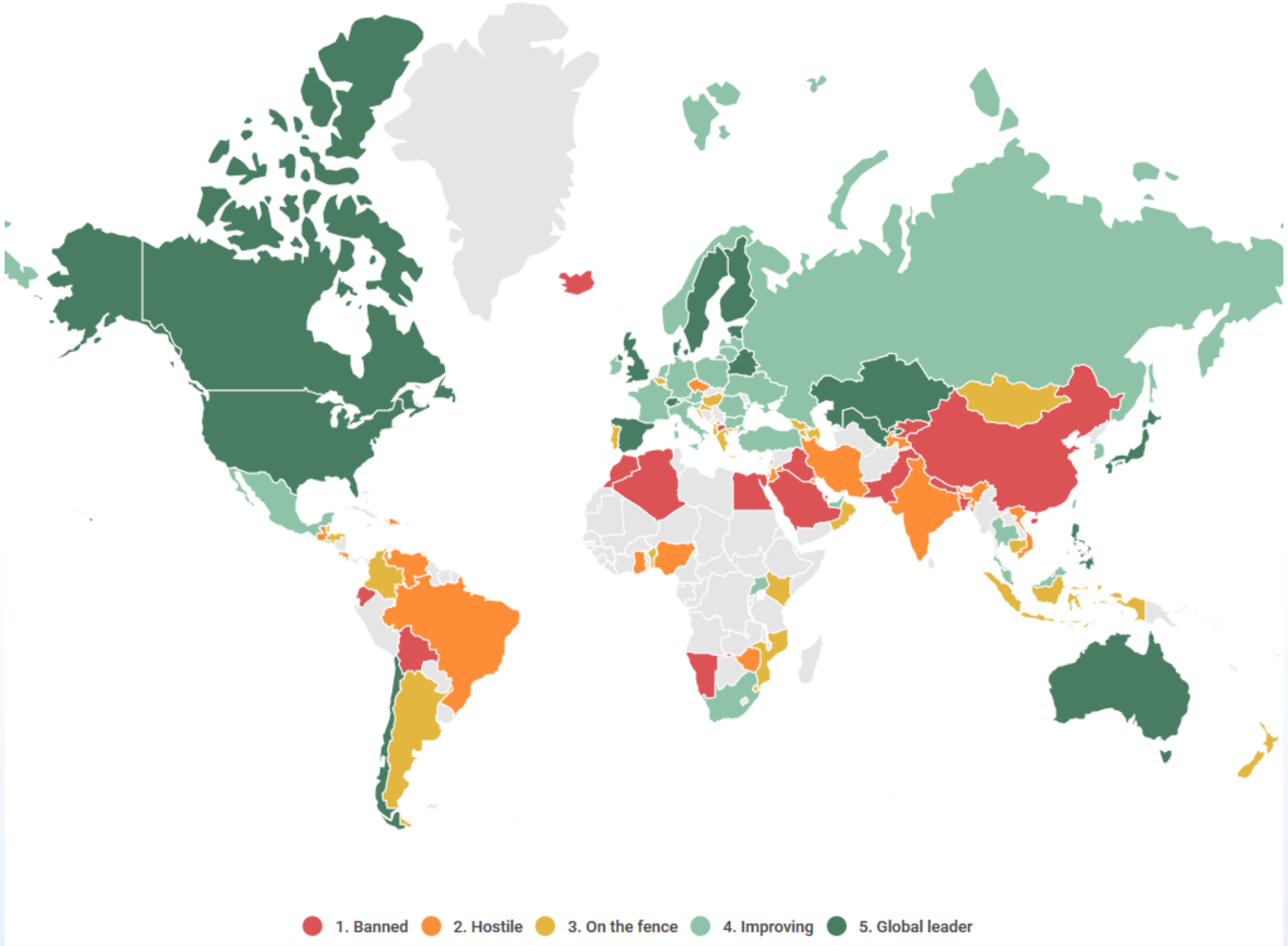


- Švicarska banka Bank Vontobel AG je leta 2016 prvič ponudila vlaganje v bitcoin
- Ripple – privatna kriptovaluta namenjena bančnim prenosom
- February 2016 je bila ustanovljena Enterprise Ethereum Alliance https://entethalliance.org/
- Na Japonskem in v Avstraliji je leta 2017 bitcoin postal uradno priznano plačilno sredstvo

- Švicarska banka Bank Vontobel AG je leta 2016 prvič ponudila vlaganje v bitcoin
- Ripple – privatna kriptovaluta namenjena bančnim prenosom
- February 2016 je bila ustanovljena Enterprise Ethereum Alliance https://entethalliance.org/
- Na Japonskem in v Avstraliji je leta 2017 bitcoin postal uradno priznano plačilno sredstvo
- November 2018 je Ohio pričel sprejemati bitcoine za plačilo davkov

- Švicarska banka Bank Vontobel AG je leta 2016 prvič ponudila vlaganje v bitcoin
- Ripple – privatna kriptovaluta namenjena bančnim prenosom
- February 2016 je bila ustanovljena Enterprise Ethereum Alliance https://entethalliance.org/
- Na Japonskem in v Avstraliji je leta 2017 bitcoin postal uradno priznano plačilno sredstvo
- November 2018 je Ohio pričel sprejemati bitcoine za plačilo davkov
- Bank of America je vložila preko 50 patentov, vezanih na blockchain in kriptovalute

- Švicarska banka Bank Vontobel AG je leta 2016 prvič ponudila vlaganje v bitcoin
- Ripple – privatna kriptovaluta namenjena bančnim prenosom
- February 2016 je bila ustanovljena Enterprise Ethereum Alliance https://entethalliance.org/
- Na Japonskem in v Avstraliji je leta 2017 bitcoin postal uradno priznano plačilno sredstvo
- November 2018 je Ohio pričel sprejemati bitcoine za plačilo davkov
- Bank of America je vložila preko 50 patentov, vezanih na blockchain in kriptovalute
- Leta 2018 s voditelji G20 soglasno sklenili, da je potrebno vzpostaviti regulacijski okvir za kripto imetja


1. Banned
2. Hostile
3. On the fence
4. Improving
5. Global leader

- Amazon Web Services v sodelovanju s Kaleido ponuja **platformo v oblaku** za integracijo blockchain rešitev z AWS storitvami.

- Walmart, Kroger, Nestle, in Unilever v sodelovanju z IBM uporabljajo blockchain za **izboljšanje kakovosti in sledljivosti hrane**.

- UN preizkuša uporabo blockchaina za **sledenje vremenskim spremembam**. Ustanovljena je bila Climate Chain Coalition.

- Tencent in Huawei vodita blockchain konzorcij Fisco, nudi uporabo **blockchain za hitre transakcije** in popoln pregled regulatorjem in avditorjem

- Toyota preizkuša blockchain za **sledenje pametnim avtomobobilom**.

- Nemška zavarovalnica Allianz je potrdila, da preizkušajo tokene za **hitrejši in cenejši prenos denarja** med podružnicami.

Družbeno

Družbeno

- Blockchain je mlad

Družbeno

- Blockchain je mlad
- Na internet je bil spuščen brez širše razlage ali predstavitve

Družbeno

- Blockchain je mlad
- Na internet je bil spuščen brez širše razlage ali predstavitve
- 90. – Nikoli ne bo mogoče globalno trgovati z nobeno valuto, za katero ne stoji centralna banka.

Družbeno

- Blockchain je mlad
- Na internet je bil spuščen brez širše razlage ali predstavitve
- 90. – Nikoli ne bo mogoče globalno trgovati z nobeno valuto, za katero ne stoji centralna banka.

KLJUB TEMU

- Ga zdaj uporabljajo in testirajo vlade, centralne banke, borze, podjetja