Zgodovina blockchaina

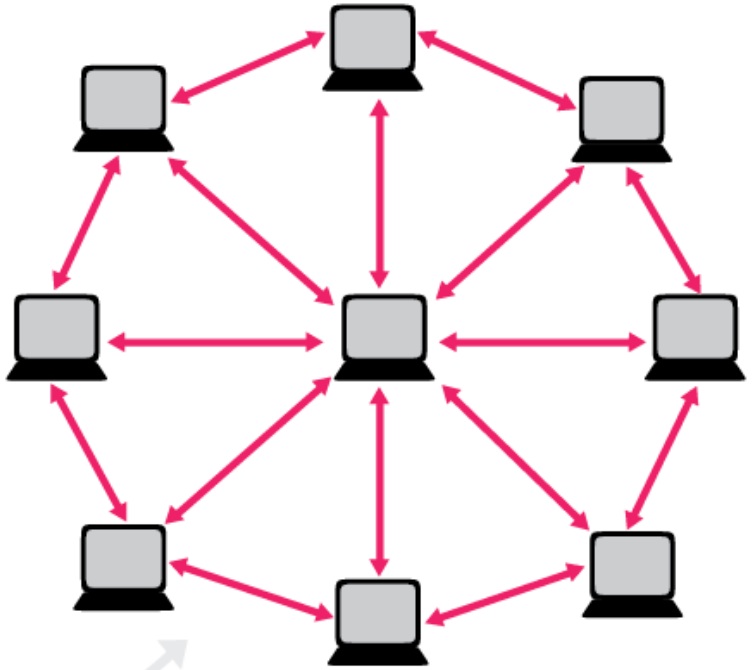
FIN-TECH Risk management delavnica

Nastja Cepak

Blockchain:

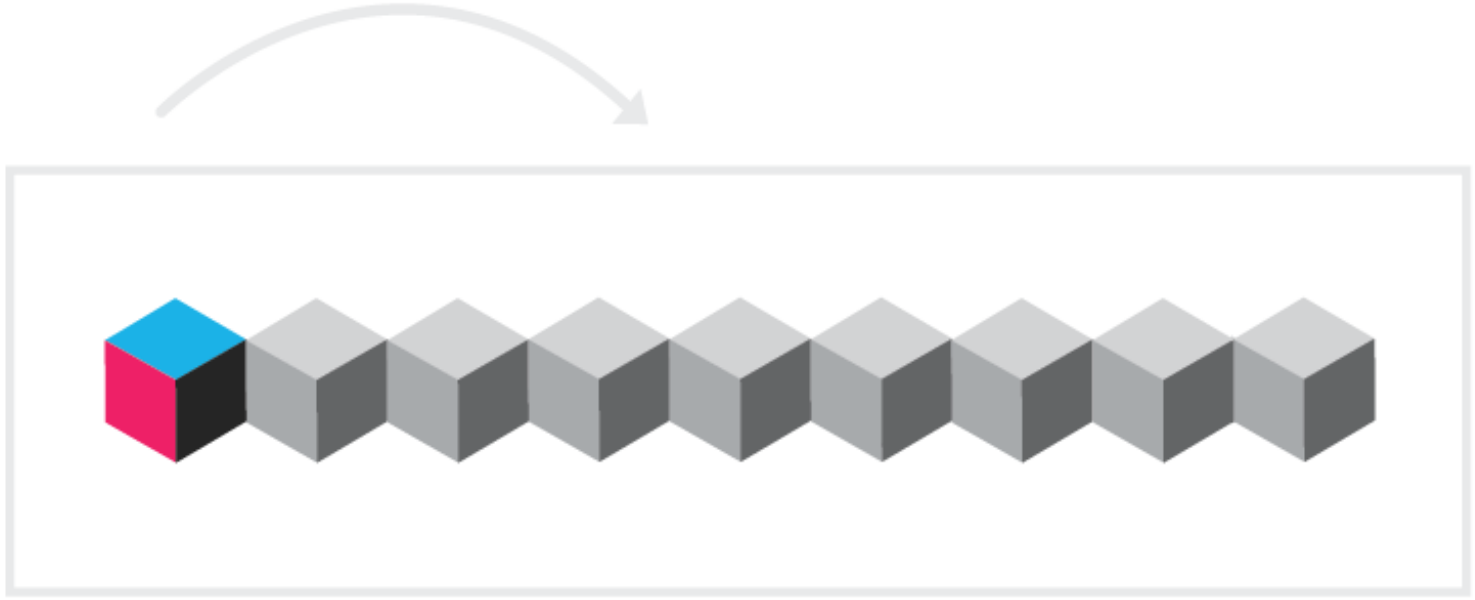
Programska baza, ki nepokvarljivo hrani naraščajočo listo transakcij.

Nekdo zahteva **transakcijo**.



Transakcija je predana **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

80. leta

1982

1985

David Chaum

- Plačila brez centralne avtoritete
- Ideja nesledljivih plačil
- DigiCash

1989

- Idejni začetki **Cypherpunk** gibanja
- Nekaj znanih članov:
  - Julian Assange
  - Številni razvijalci TOR brskalnika
  - Satoshi Nakamoto

90. leta

1991

1992

1993

1996

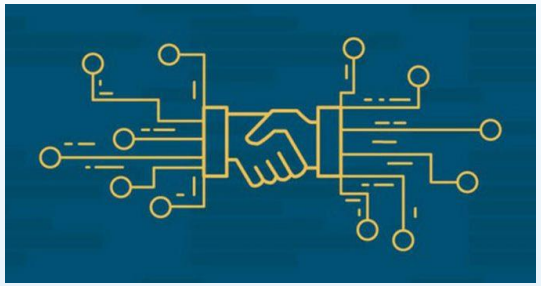
1999

Razvijali koncepte in reševali probleme:

- **KDAJ** je bil document narejen: timestamping
- Kako več dokumentov združiti v **EN BLOK**: Merklova drevesa
- Kako varno, necetralizirano **POTRJEVATI TRANSAKCIJE**: Proof of work

Prvi Cypherpunk manifesto

Predstavljena ideja pametnih pogodb



200x

2002

2004

2005

- Prva implementacija **Ripple** projekta

Adam Back

- Dectralizirana omrežja in zaupanje
- Hashcash (PoW)

2008

2009

Uradno predstavljen in implementiran prvi **blockchain**

2008-2009

Zakaj pomembna prelomnica?

Prvič je bil rešen “double spending” problem z uporabo peer-to-peer omrežja.

18. avgust, 2008 Registrirana domena bitcoin.org

31. oktober, 2008 **Satoshi Nakamoto** na Cypherpunk mailing listi objavi članek “Bitcoin: A Peer-to-Peer Electronic Cash System” https://bitcoin.org/bitcoin.pdf

3. januar, 2009 Potrjen prvi blok prvega blockchaina

Satoshi Nakamoto

Kdo?

Kaj/Kateri?

```
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._¬....
```

Potrjevanje transakcij

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

- Potrjevanje poteka z uporabo **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

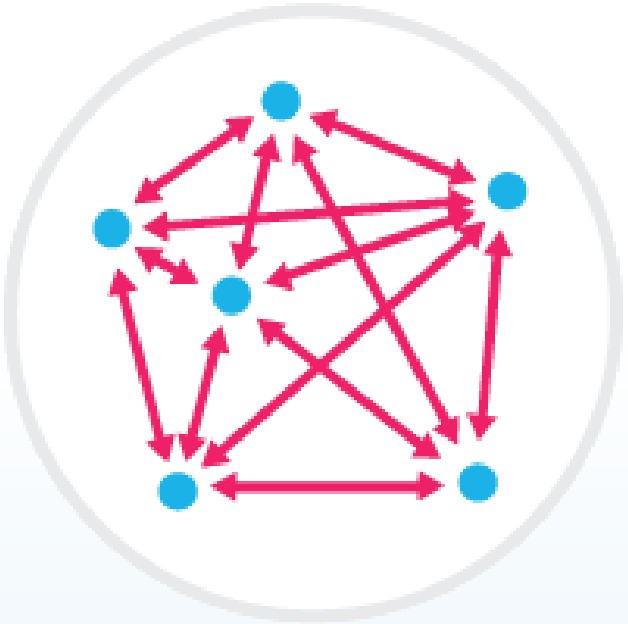
00…0xy…z

najti 

=

potrditi transakcijo

Kdo potrjuje transakcije?



https://www.blockchain.com/

2009

12. januar, 2009

Na Bitcoin blockchainu je zabeležena **1. transakcija**:
Hal Finney – Satoshi Nakamoto
povezava

29. junij, 2009

Kitajska **prepove** trgovanje virtualnih valut za izdelke.

5. oktober, 2009

New Liberty Standard na podlagi cene elektrike objavi **menjalni tečaj**: 1USD = 1309.03BTC
povezava

30. december, 2009

Prvo povišanje **težavnosti** rudarjenja.

2010

8. februar, 2010 Odpre se prva **Bitcoin menjalnica** – Bitcoin Market.

2011-09-10 17:36:27

Signup | Login

Pair	Last	Change*	Volume*

*Based on the last 24 hours

Home | Membership | Top Orders | Recent Trades | Charts | Resources & Tools

Featuring:

- ***Automated & Escrow Trading***
- ***Multiple Payment Processors***
- ***On-site Rating & Private Messaging***

BMBTC/BMUSD

Flash Player Required

News

2011-6-7 BMBTC/PPUSD Update

We were able to seize about 5 BTC from the fraudulent accounts. This is roughly equivalent to the sum of the transaction fees charged on these trades. Therefore, we've decided to issue transaction **fee** refunds on all fraudulent transactions. We realize this is a small compensation, but it is the fairest form of distribution that we can imagine. Members should see the

2010

8. februar, 2010 Odpre se prva **Bitcoin menjalnica** – Bitcoin Market.

18. maj, 2010 **Prvi nakup** dobrine z Bitcoinom – Pizza Day
https://bitcointalk.org/index.php?topic=137.msg1195#msg1195

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

2010

8. februar, 2010 Odpre se prva **Bitcoin menjalnica** – Bitcoin Market.

18. maj, 2010 **Prvi nakup** dobrine z Bitcoinom – Pizza Day
https://bitcointalk.org/index.php?topic=137.msg1195#msg1195

17. julij, 2010 Menjalnica **MtGox** začne trgovati z Bitcoini.

8. avgust, 2010 “The "value out" in this block #74638 is **quite strange**.”
https://bitcointalk.org/index.php?topic=822.0

2011

9. februar, 2011 BTC doseže vrednost 1USD.

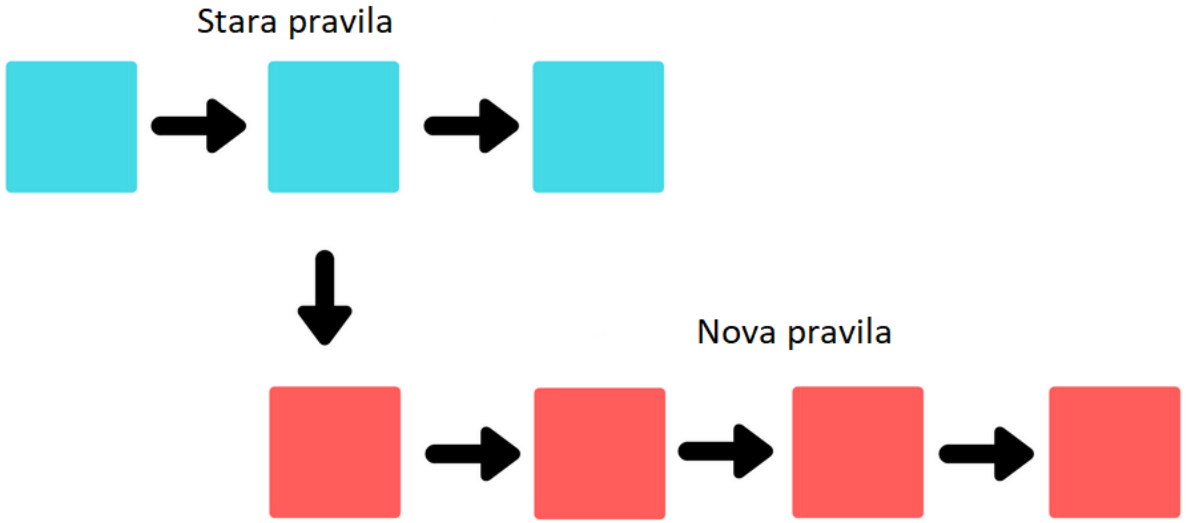
februar, 2011 Odpre se prva spletna stran **Silk Road.**

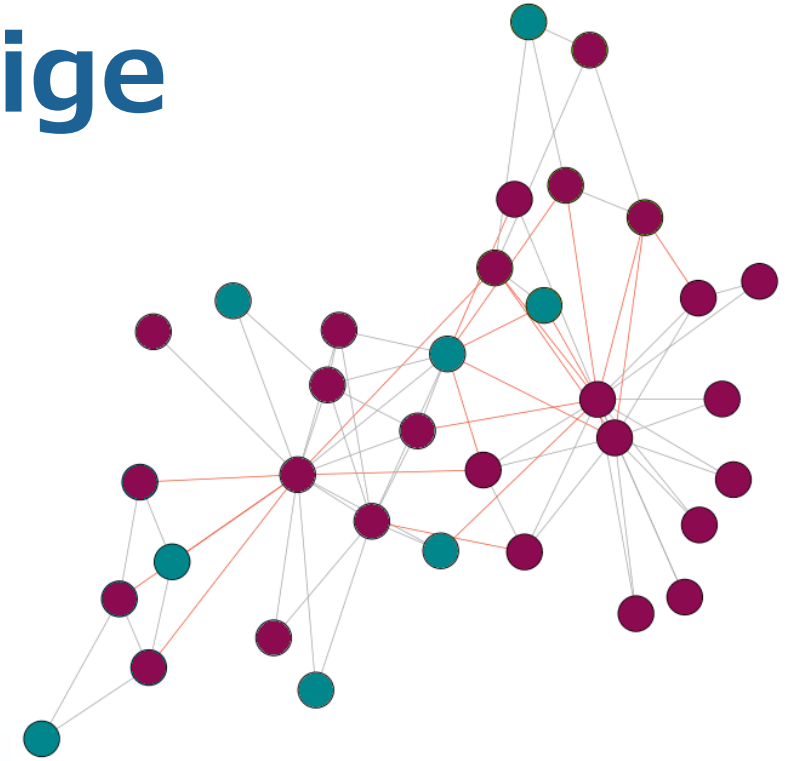
23. april, 2011 BTC doseže vrednost 1EUR/GBP.

24. junij, 2011 Težavnost rudarjenja BTCja je za 10x povečana.

29. avgust, 2011 Predlagan prvi **BIP** – “Bitcoin Improvement Proposal”

Cepljenje verige





Soft fork	Hard fork
Strožja pravila	Razširjena/spremenjena pravila
Kompatibilno s starejšo kodo	Nekompatibilno s starejšo kodo
Stara vozlišča sprejemajo nove bloke	Stara vozlišča ne sprejemajo novih blokov

2011

9. februar, 2011 BTC doseže vrednost 1USD.

februar, 2011 Odpre se prva spletna stran **Silk Road.**

23. april, 2011 BTC doseže vrednost 1EUR/GBP.

24. junij, 2011 Težavnost rudarjenja BTCja je za 10x povečana.

29. avgust, 2011 Predlagan prvi **BIP** – “Bitcoin Improvement Proposal”

Satoshi Nakamoto prepusti razvijanje kode drugim in se umakne.

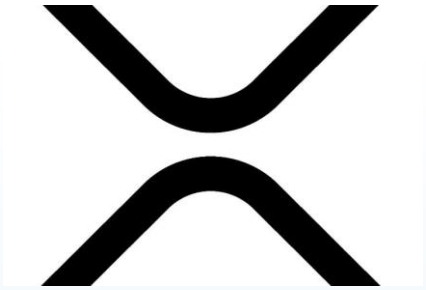
Pojav **altcoinov** (Namecoin, Litecoin, Swiftcoin)

Altcoin

Kriptovaluta, ki ni Bitcoin.

Ethereum

Monero



Ripple

Bitcoin Cash

Trumpcoin

Litecoin

2012

januar, 2012

Začetki širše **medijske pozornosti**:
“The Good Wife” – Bitcoin for Dummies

Začetek kriptovalute Tether (USDT).

september, 2012

Ustanovljen Bitcoin Foundation.

Ustanovljeno OpenCoin podjetje, ki razvija Ripple protokol.

Razvija se zavedanje o **raznih načinih uporabe** blockchaina.


From
Apr 28, 2013
To
Dec 31, 2014
Market Cap
$10B
$5B
$0
Price (USD)
$1,600.00
$800.00
$0
24h Vol
0
Jul '13
Oct '13
Jan '14
Apr '14
Jul '14
Oct '14

2013

Prvi veliki bitcoin pohod, države sprejemajo regulacije, številne spletne strani začnejo sprejemati bitcoine.

marec, 2013 Problem s posodobitvijo Bitcoin kode z verzije 0.7 na 0.8.

oktober, 2013 FBI zapre ustnovitelja Silk Road, zapre spletno stran in zaseže Bitcoine.

Odprt prvi Bitcoin bankomat – Vancouver, Kanada.

november, 2013 Vrednost bitcoina prvič doseže **vrednost 1000USD**.

Vitalik Buterin objaci whitepaper Ethereuma.

Silk Road

Ross William Ulbricht,
“Dread Pirate Roberts”

- Takrat največji črni trg, eden prvih sodobnih **darknet** trgov.
- Trgoval predvsem z drogami.
- FBI zasegel 144,336 bitcoinov in jih prodal na dražbah v 2014 in 2015
- November 2013:
  Silk Road 2.0

Zasegli bitcoine = zasegli **ključe denarnic**

SILK ROAD PAYMENT SYSTEM

Buyer exchanges currency for BTC

EXCHANGER

Buyer transfers BTC to SR account

BUYER

Buyer makes purchase

BTC held in escrow until order finalized

Silk Road takes commission

Vendor is paid

Vendor exchanges BTC for currency

EXCHANGER

Vendor moves BTC from SR account

VENDOR

GOVERNMENT EXHIBIT 113 A
14 Cr. 68 (KBF)

2013

Prvi veliki bitcoin pohod, države sprejemajo regulacije, številne spletne strani začnejo sprejemati bitcoine.

marec, 2013 Problem s posodobitvijo Bitcoin kode z verzije 0.7 na 0.8.

oktober, 2013 FBI zapre ustnovitelja Silk Road, zapre spletno stran in zaseže Bitcoine.

Odprt prvi Bitcoin bankomat – Vancouver, Kanada.

november, 2013 Vrednost bitcoina prvič doseže **vrednost 1000USD**.

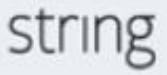
Vitalik Buterin objaci whitepaper Ethereuma.

Vitalik Buterin

- Rojen 1994 v **Rusiji**, leta 2000 se preselil v **Kanado**.
- 2011 se pričel zanimati za blockchain, pisal za **Bitcoin Weekly** in so-ustanovil **Bitcoin Magazine**.
- 2013 potoval po svetu, spoznaval blockchain projekte -> **Ethereum**

- **Enterprise Ethereum Allian**ce, razvoj pametnih pogodb
- Srečanje s Putinom, sodelovanje s Kitajsko.
- Lažna poročila o smrti, vpliv na Ethereum ceno.

LAUNCH MEMBERS



2013

marec, 2013	Finančno ministrstvo ZDA izda **smerice** za decentralizirane virtualne valute.
maj, 2013	Zvezno sodišče ZDA izda mnenje, da je bitcoin **valuta** oziroma oblika **plačilnega sredstva**.
julij, 2013	Tajska **prepove** uporabo kriptovalut, vključno z bitcoinom.
avgust, 2013	Nemško ministrstvo za finance izda smernice, ki pravijo, da bitcoin sicer ni e-denar, je pa **finančni instrument**.
december, 2013	Kitajska bankam **prepove** trgovanje z Bitcoinom.


From
Apr 28, 2013
To
Dec 31, 2014
Market Cap
$10B
$5B
$0
Price (USD)
$1,600.00
$800.00
$0
24h Vol
0
Jul '13
Oct '13
Jan '14
Apr '14
Jul '14
Oct '14

2014

Bitcoine začnejo sprejemati: **Microsoft digital goods, Dell**, Newegg, Expedia, Zynga, Overtstock.com,…

marec, 2014

Internal Revenue Service ZDA opozarja - pri davčni napovedi je potrebno poročati o prihodkih, vezanih na prodajo kriptovalut!

Philip in Diana Koshy – sledenje bitcoin transakcijam

maj, 2014

Menjalnica MtGox oznani bankrot.

MtGox

- Že leta 2011 dve manjši kraji preko računalnikov auditerjev – hot wallets.
- Med 2013 in 2014 je preko MtGox potekalo 70% vseh bitcoin transakcij.

- Ukradenih **744.000 + 100.000** bitcoinov podjetja (več kot 7% vseh bitcoinov v obtoku).
- Vse trgovanje je bilo ustavljeno in MtGox je na Japonskem prijavil bankrot.
- Vdor v računalnike MtGox že leta 2011, sledila neprestana, počasna kraja.

2014

Bitcoine začnejo sprejemati: **Microsoft digital goods, Dell**, Newegg, Expedia, Zynga, Overtstock.com,…

marec, 2014

Internal Revenue Service ZDA opozarja - pri davčni napovedi je potrebno poročati o prihodkih, vezanih na prodajo kriptovalut!

Philip in Diana Koshy – sledenje bitcoin transakcijam

maj, 2014

Menjalnica MtGox oznani bankrot.

junij, 2014

V manj kot 6 mesecih se težavnost rudarjenja podeseteri.

julij, 2014

Prične se predprodaja **Ethereuma**.

september, 2014

Ameriška komisija prvič **odobri finančni produkt**, baziran na bitcoinu: TeraExchange – trgovanje z bitcoin derivativi
povezava

2015

januar, 2015 **Bitstampu** ukradejo 19.000 bitcoinov.

marec, 2015 Britanska vlada objavi rezultate javnega poziva za zbiranje informacij o blockchainu.

avgust, 2015 **Barclays Bank** postane prva velika banka, ki sprejema bitcoine.

september, 2015 9 finančnih institucij ustanovi **R3 konzorcij**.

CFTC določi, da so virtualne valute **blago oz. surovina** (commodity).

Debata o posodobitvi bitcoin blockchaina: velikost blokov in Segregated Witness

2016

Začne se sprejemanje bitcoina po celotni Latinski Ameriki.

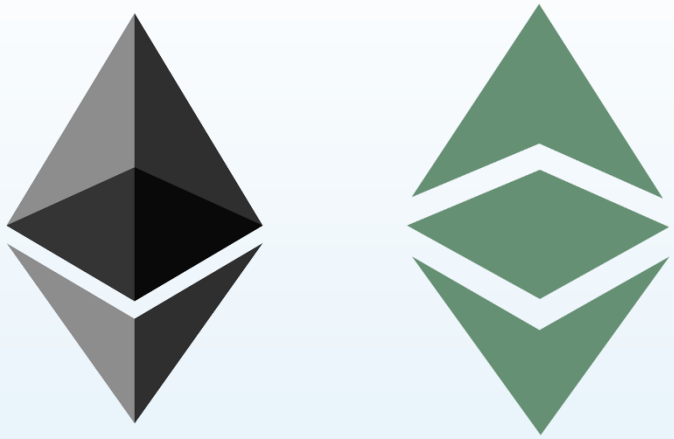
marec, 2016 Japonska prizna bitcoin kot „podobnega pravemu denarju“.

julij, 2016 Raziskava: od leta 2013 je gonilo bitcoina zakonita trgovina https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2808762

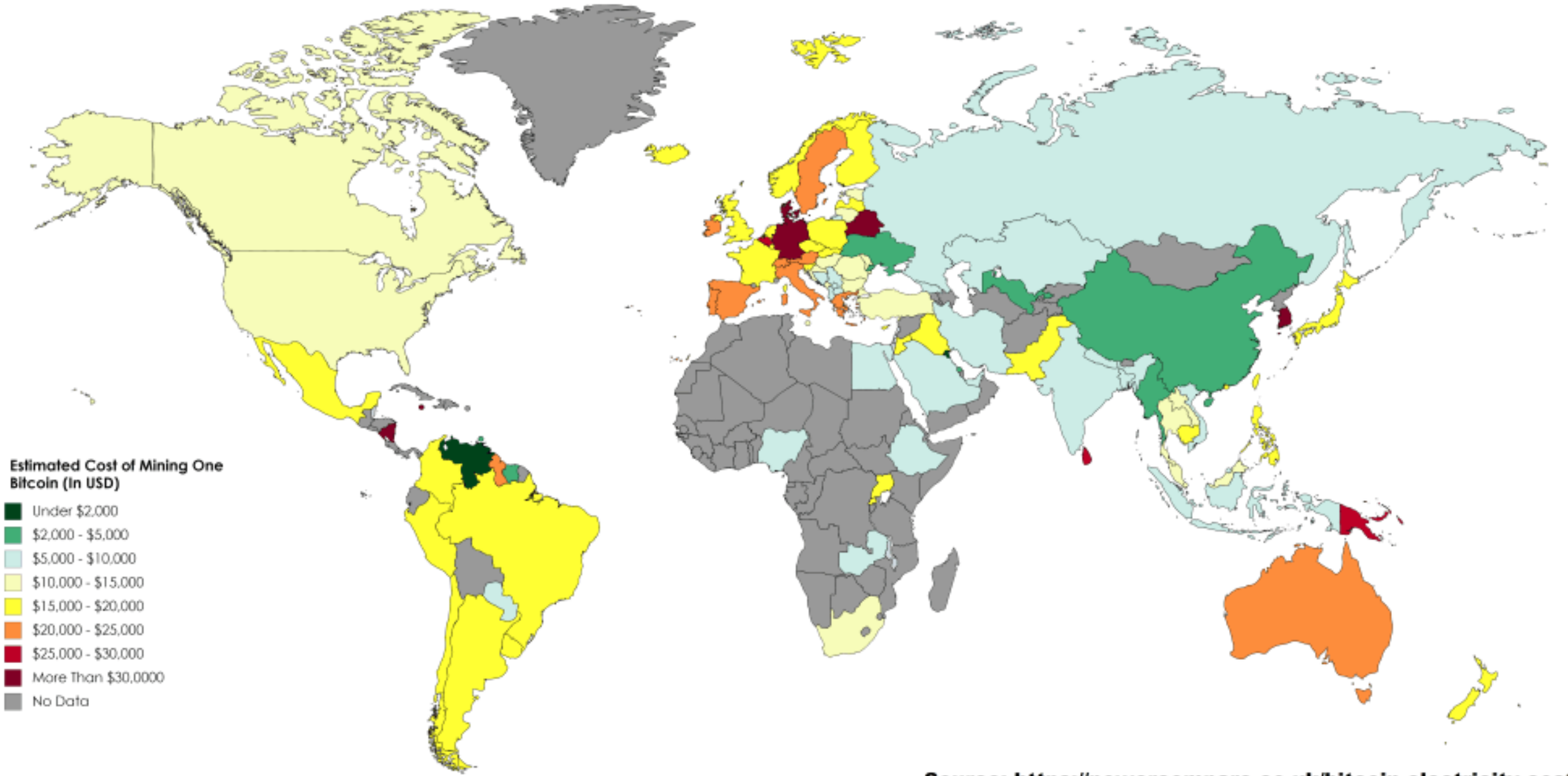
junij - julij, 2016 DAO napad, ki sproži Ethereum cepitev.

avgust, 2016 **Bitfinexu** ukradejo 120.000 bitcoinov.

september, 2016 BTC.com odpre danes največji mining pool.

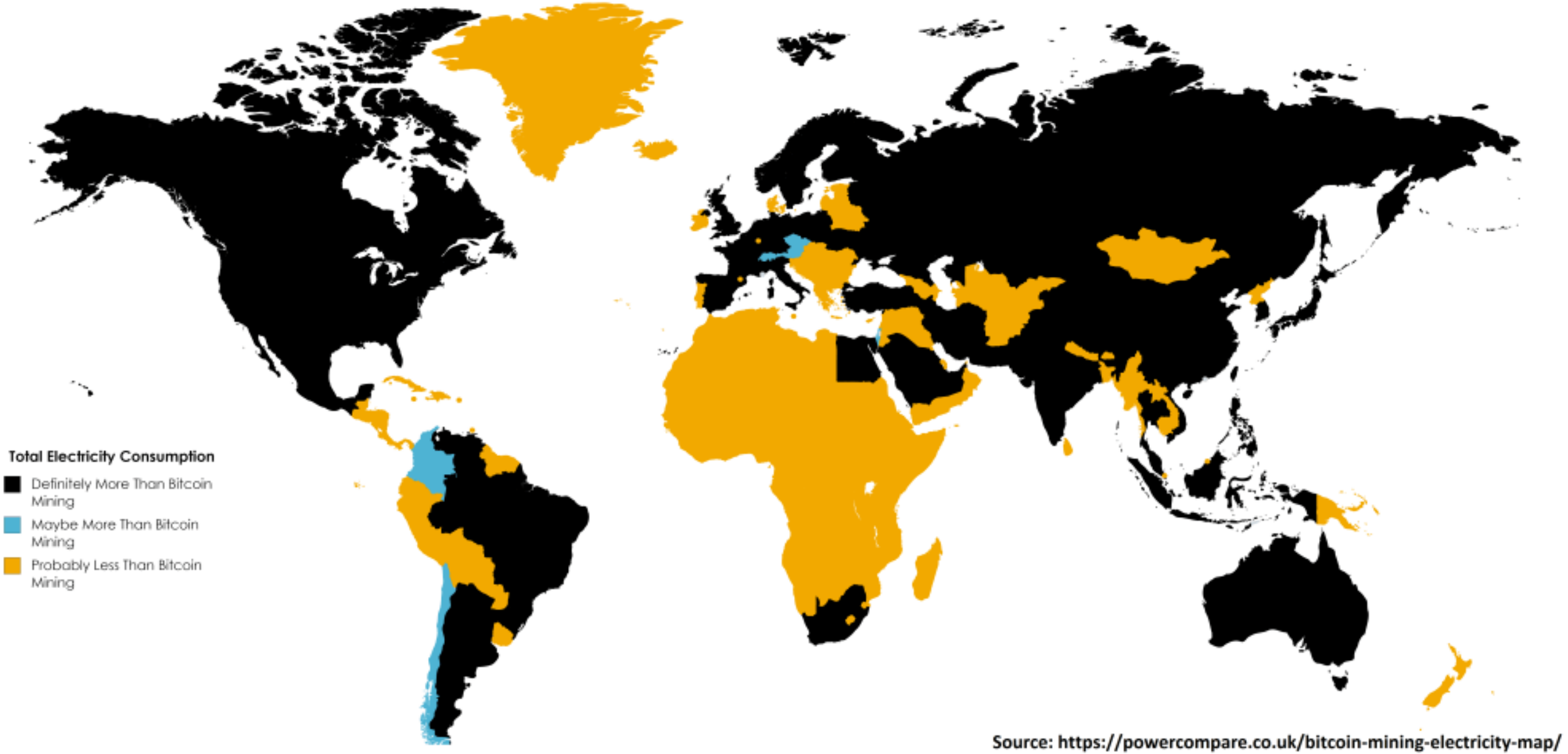


Estimated Electricity Cost Of Mining One Bitcoin By Country



Source: https://powercompare.co.uk/bitcoin-electricity-cost/

Countries That Consume More Or Less Electricity Than Bitcoin Mining In Late 2018



Source: https://powercompare.co.uk/bitcoin-mining-electricity-map/


From
Dec 29, 2016
To
May 16, 2019
Market Cap
$240B
$120B
$0
Price (USD)
$16,000.00
$8,000.00
$0
24 h Vol
0
Jan '17
May '17
Sep '17
Jan '18
May '18
Sep '18
Jan '19
May '19

2017

april, 2017 Japonska prizna kriptovalute kot “legal property”.

maj, 2017 Poloniex - 640% narast transakcij v 4 mesecih

junij, 2017 Testiran prvi blockchain, odporen na napade s **kvantnim računalnikom**.

avgust, 2017 S SegWit cepitvijo se Bitcoin razcepi na Bitcoin in **Bitcoin Cash**.

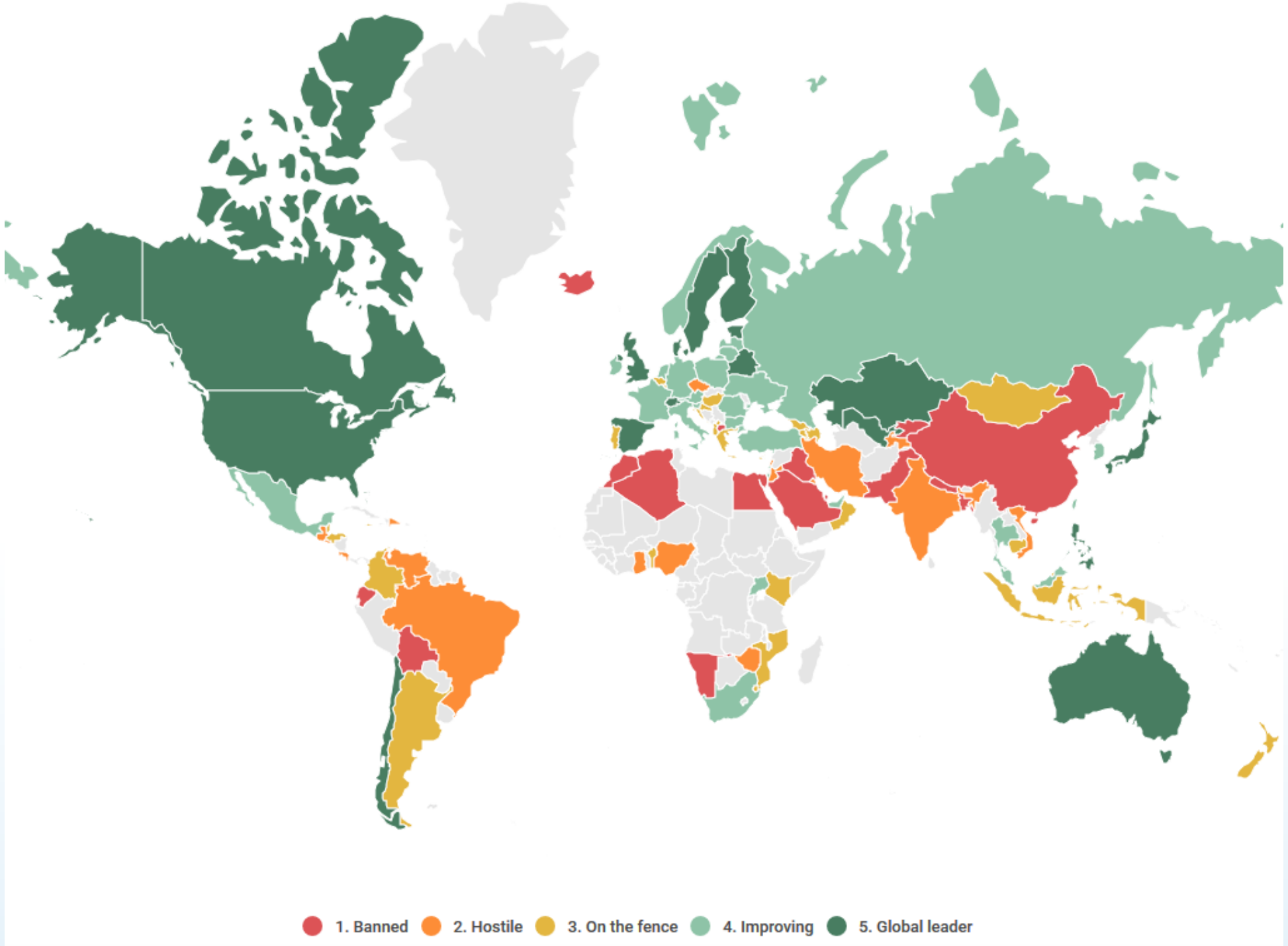
september, 2017 Južna Koreja prepove ICO, Kitajska jih začasno zaustavi.

november, 2017 Vsaj 3 finančne skupine pričnejo s trgovanjem v **bitcoin futures**.

2018

ICO zamirajo, prepovedi oglaševanja kriptovalut (Facebook, Google,...), nekatere banke prepovejo izposojo denarja za nakup kriptovalut, strožja identifikacija na borzah.

september, 2018	Japonsko mesto Tsukuba prvo preizkusi **volilni sistem**, baziran na blockchainu.
oktober, 2018	G20 pozove k regulaciji kripto trga.
november, 2018	Ohio sprejema plačilo davkov v Bitcoinih.
december, 2018	Bank of America do sedaj vložila že 50 blockchain patentov.


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

Privatni sektor

- 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.