

A 40.000.000 DOLLÁROS PIZZA TÖRTÉNETE, AVAGY MENNYIT ÉR A BITCOIN?



Sándor Barnabás
biztonságtechnikai mérnök, etikus hacker

Budapest, 2019. március 19.

Péztörténet



BARTER



GOLD



**METALL
COINS**



**PAPER
MONEY**



**PLASTIC
CARDS**



**ELECTRONIC
MONEY**



**CRYPTO
CURRENCY**

Időutazás



[thefacebook]

2004



2007

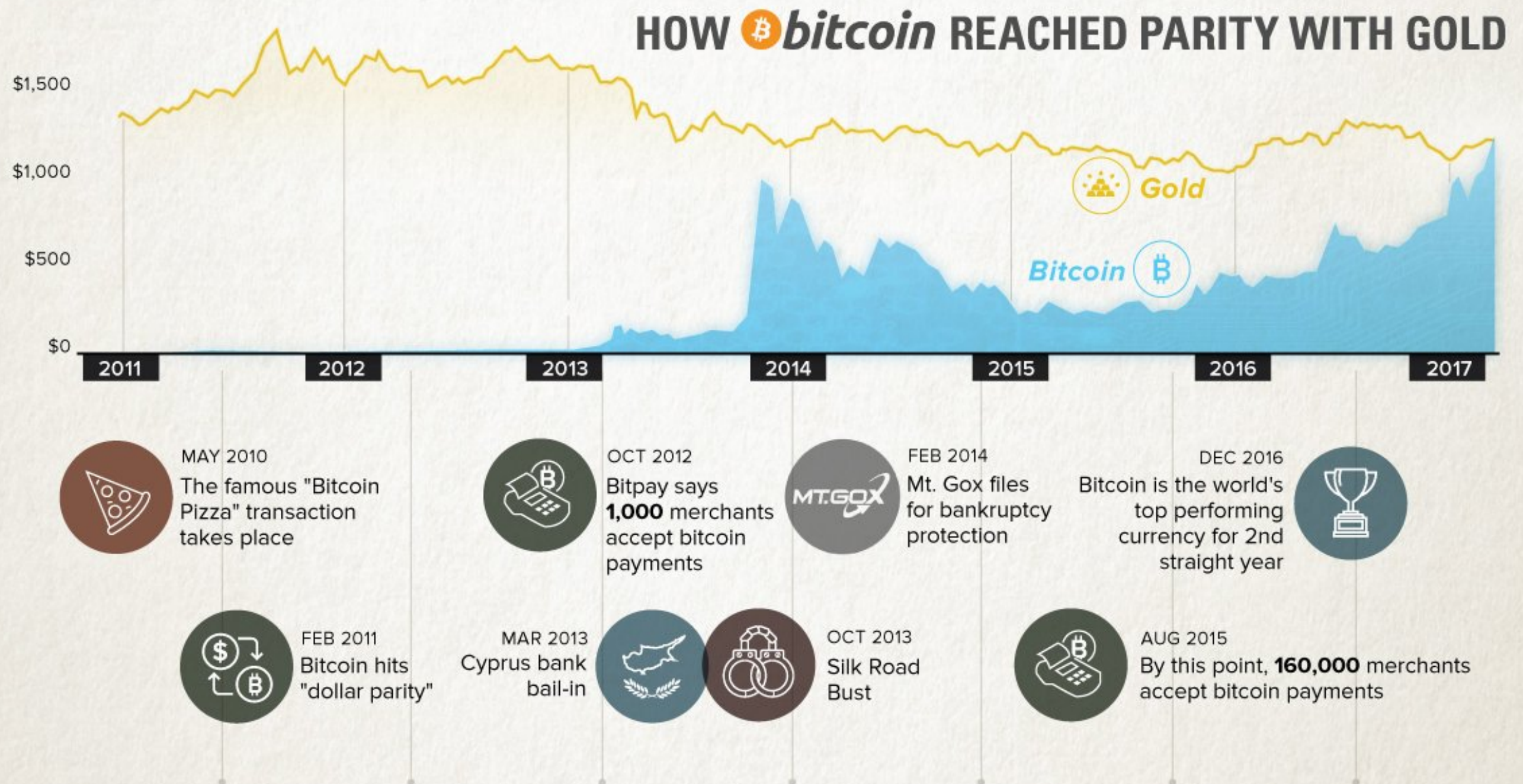


2009

BITCOIN'S 10th ANNIVERSARY



Bitcoin története



Forrás: <https://twitter.com/VisualCap/status/837770240507392001>

Bitcoin árfolyam





COINTELEGRAPH



Hanyecz László

laszlo

Full Member



Activity: 199

Merit: 330



Re: Pizza for bitcoins?

May 22, 2010, 07:17:26 PM

Merited by *xtraelv* (1)

I just want to report that I successfully traded 10,000 bitcoins for pizza.

Pictures: <http://heliacal.net/~solar/bitcoin/pizza/>

Thanks jercos!

BC: 157fRrqAKrDyGHR1Bx3yDxeMv8Rh45aUet

sirius

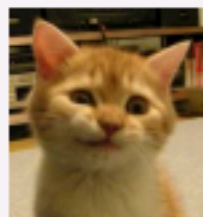
Bitcoiner

Sr. Member



Activity: 429

Merit: 253



Re: Pizza for bitcoins?

May 22, 2010, 10:10:25 PM

Congratulations laszlo, a great milestone reached 🎉

Identifi - Decentralized address book with trust ratings

I'm not a forum admin - please contact [theymos](#) instead.

Forrás: <https://bitcointalk.org/index.php?topic=137.msg1195#msg1195>

Blokklánc technológia

Blokklánc technológia

Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary

Address [18icUDPfM9FwiizxQWqXL4DDMXBrydwSrV](#)

Hash 160 [54a78b09bd9441fd63a3b914410c329b1b36e6b6](#)

Tools [Related Tags](#) - [Unspent Outputs](#)

Transactions

No. Transactions 2

Total Received **\$ 62.80**

Final Balance **\$ 0.00**

[Request Payment](#)

[Donation Button](#)



Received Transactions (Oldest First)

[Filter](#) ▼

[2ede37015c9e721b37ff99d6981d0c6c3da2ac9b32d436cdacfaa518d0b39f56](#)

(Fee: \$ 12.14 - 79.34 sat/WU - 317.35 sat/B - Size: 521 bytes) 2017-12-11 17:16:44

[1CubJHEz6NB6KPS2cYRQwJj6kU1RpFPPzt](#) (\$ 63.86 - Output)

[1BpfgasyATMwhArudq25criG2i22yrAHUw](#) (\$ 99.35 - Output)

[1QLGY3182FTV2pLPir3k5JXx6ZVb2fgAp](#) (\$ 11.77 - Output)



[1G354ZyHwxrVuZ4G59DjL9ZhCA2QWetYK6](#) - (Spent)

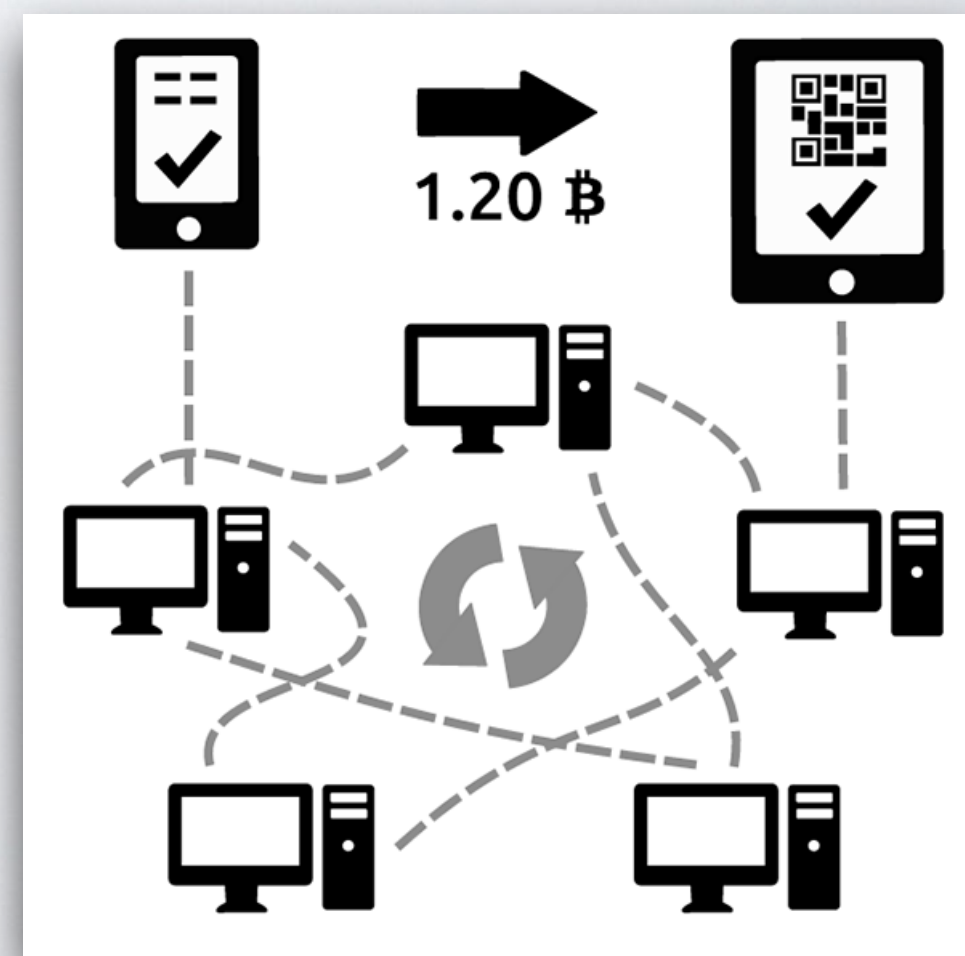
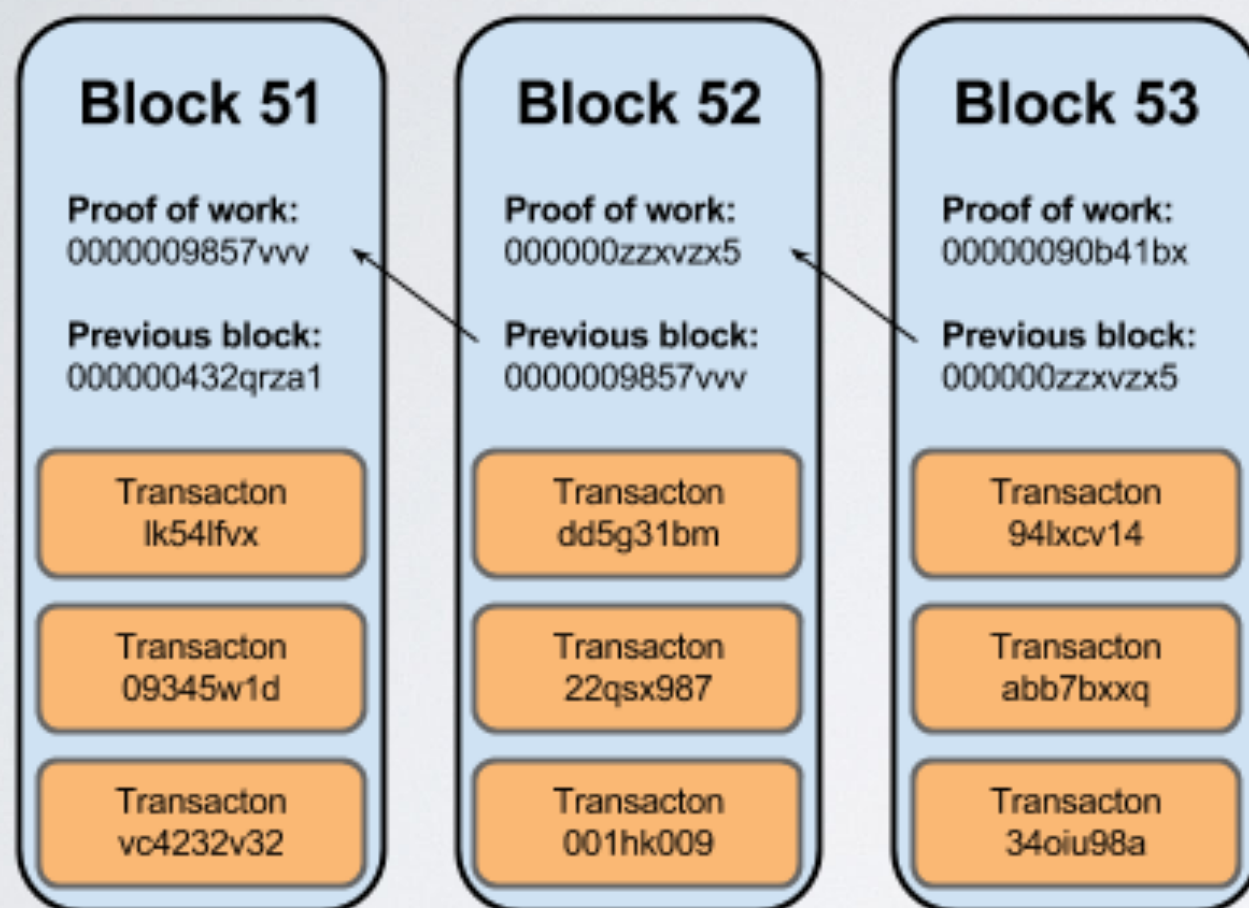
\$ 100.05

[18icUDPfM9FwiizxQWqXL4DDMXBrydwSrV](#) - (Spent)

\$ 62.80

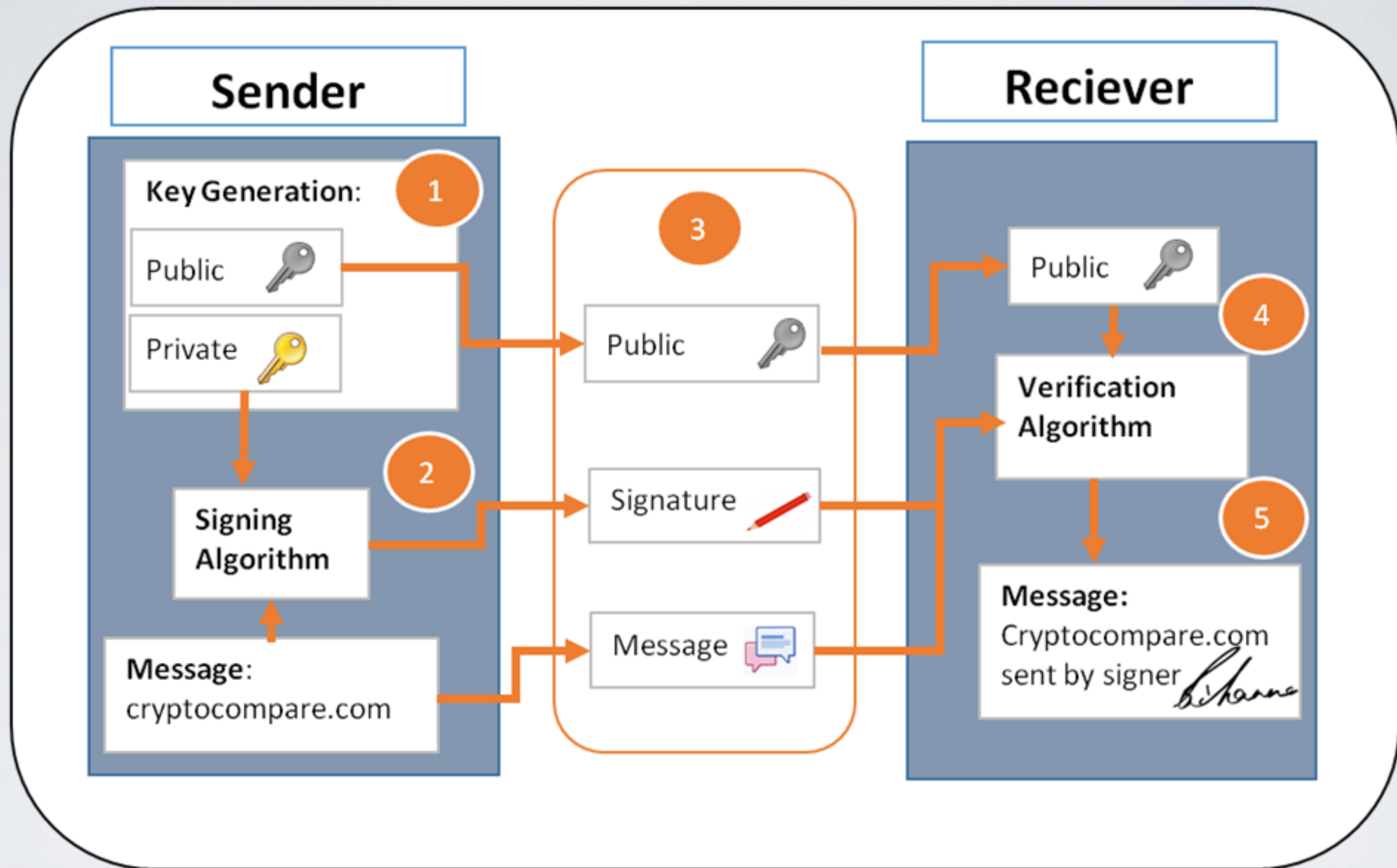
\$ 62.80

Blokklánc technológia



Titkosítás és tárolás

Titkosítás



Forrás: www.cryptocompare.com

Tárolás

Hot wallet

A cég tárolja a Privát kulcsot a szerverein.

Előny:

- Gyors hozzáférés
- Kereskedés esetén gyors hozzáférés

Hátrány:

- Privát kulcsot a cég tárolja
- Kompromittálódás esetén, elveszhetnek a koinok

Cold wallet

A privát kulcs saját, fizikai eszközünkön tároljuk.

Előny:

- Nálunk van a privát kulcs
- Internettől független

Hátrány:

- Lassabb hozzáférés
- Kompromittálódás esetén, elveszhetnek a koinok

Trezor vs Ledger



Tárolás

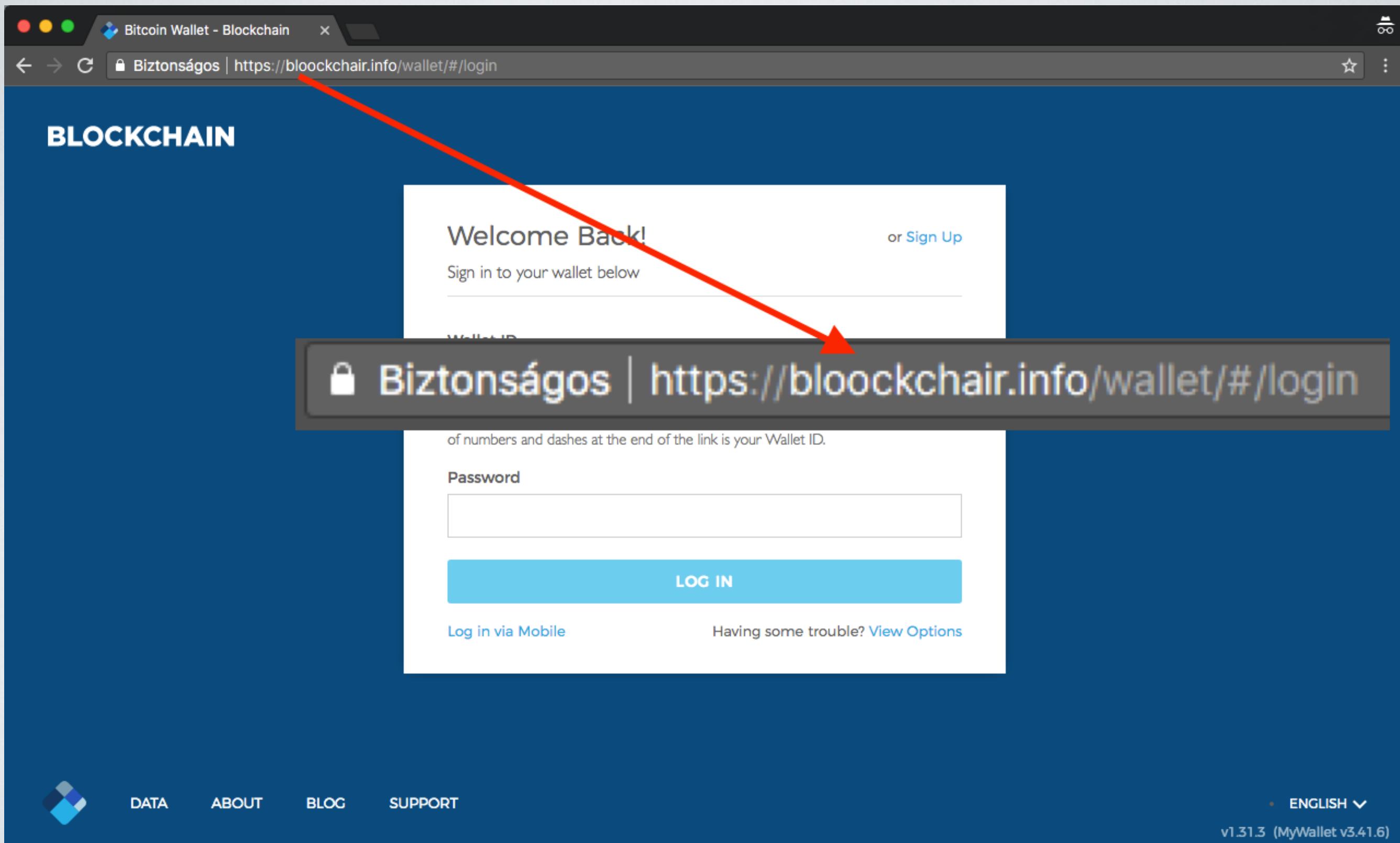
Biztonsági problémák

- Visszaállítási szavak elvesztése esetén, hozzáférés szerezhető az eszköz felett
- Amennyiben megsemmisül az eszköz és a visszaállítási szavak, úgy nem tudunk hozzáférni az eszközhöz
- Elhanyagolt firmware frissítés esetén biztonsági kockázat



Biztonságtudatosági javaslatok

Támadási módszerek

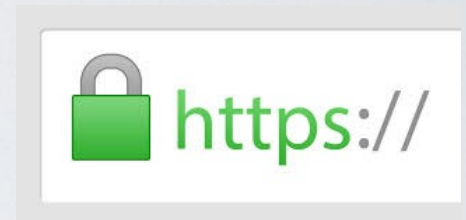


Biztonságtudatossági javaslatok

- Nyilvános vezeték nélküli hálózatok kerülése



- Titkosított kapcsolattal való böngészés



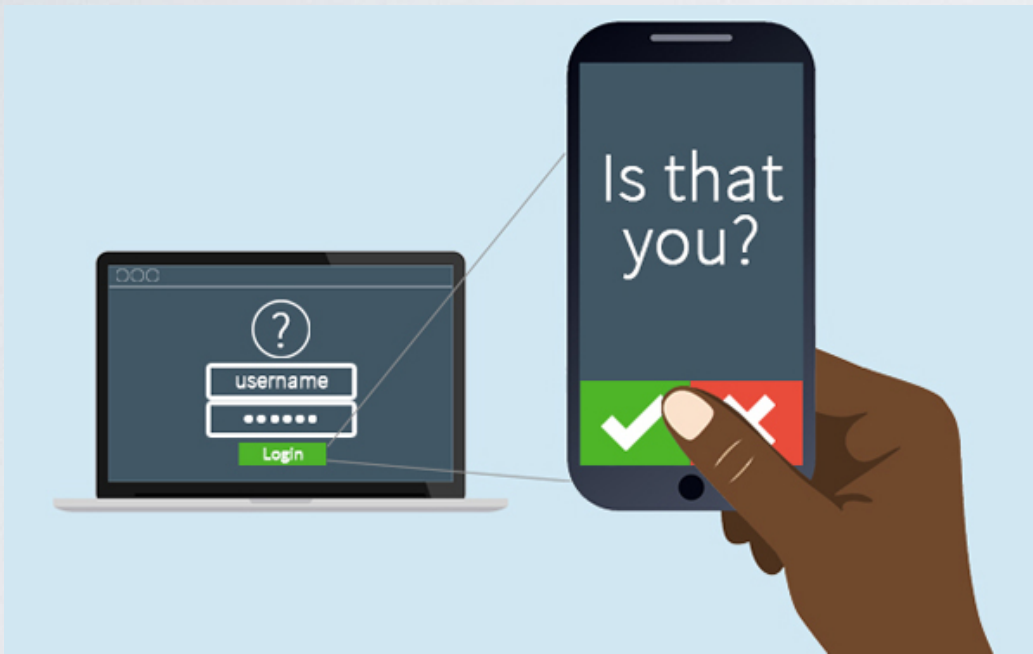
- Jelszavak biztonsága

- Minimum 15 karakter hosszú jelszó használata
- Kis,- nagybetű, szám, speciális karakter használata
- Ne használjunk egy jelszót több helyre
- Folyamatosan cseréljük
- Ne írjuk fel sehova!



Biztonságtudatossági javaslatok

- Kétlépcsős azonosítás



Google Authenticator settings

Active



Description

Henrik Schacks blog

Description you'll see on your phone.

Secret

5YGQ4IAR32CYA6PY

Create new secret

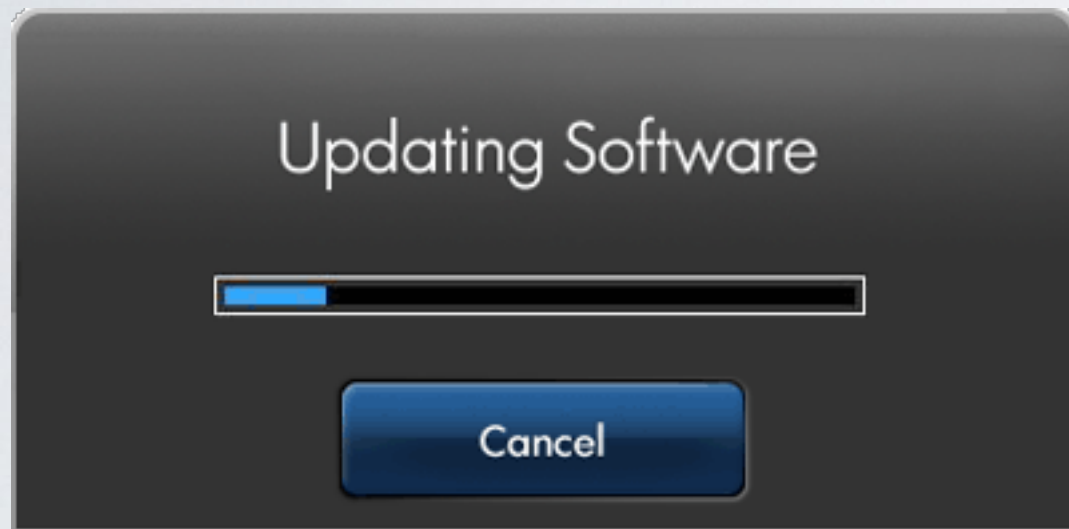
Show/Hide QR code



Scan this with the Google Authenticator app.

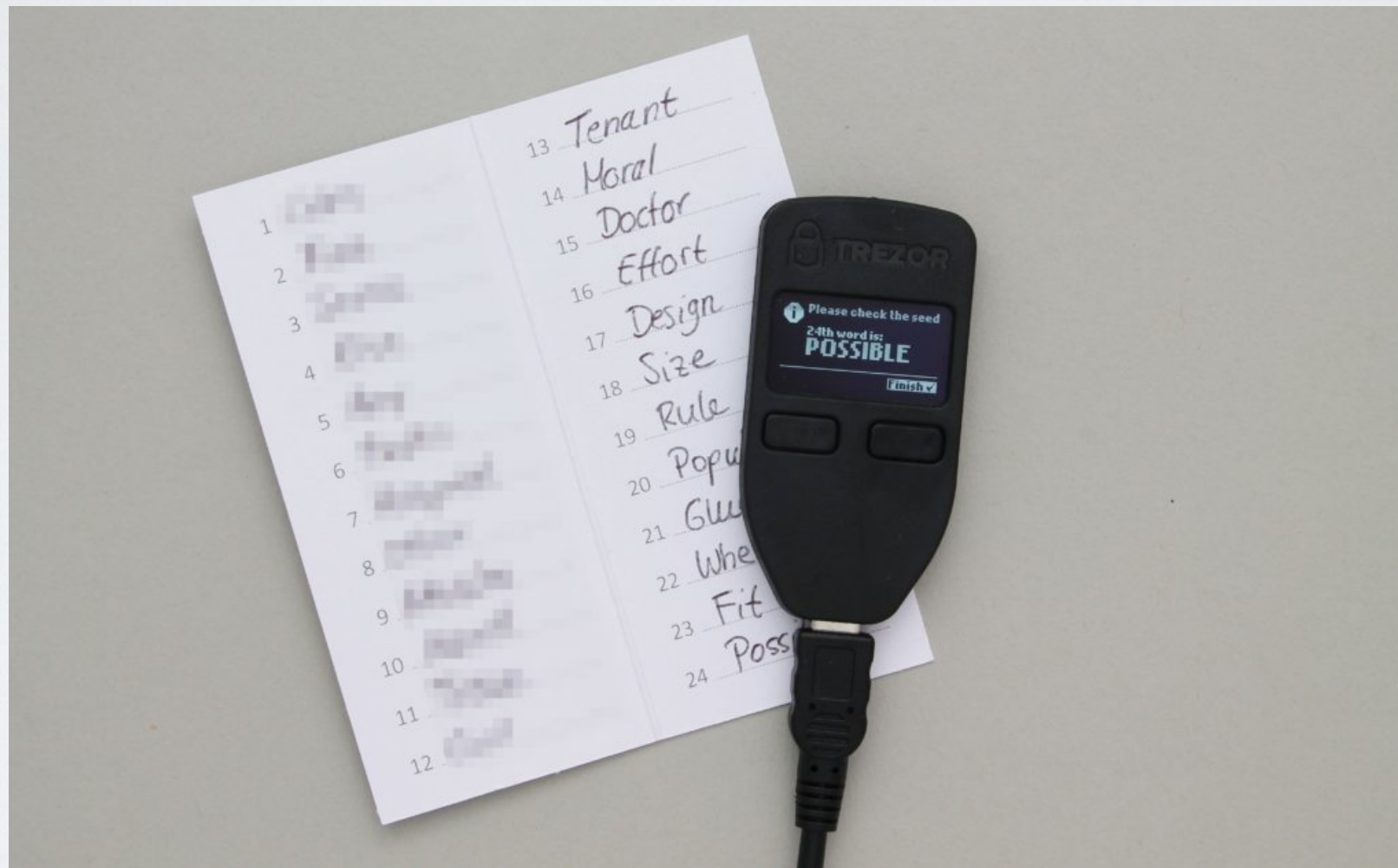
Biztonságtudatossági javaslatok

- Folyamatos szoftver és firmware frissítés



Biztonságtudatossági javaslatok

- Visszaállítási szavak biztonságos tárolása



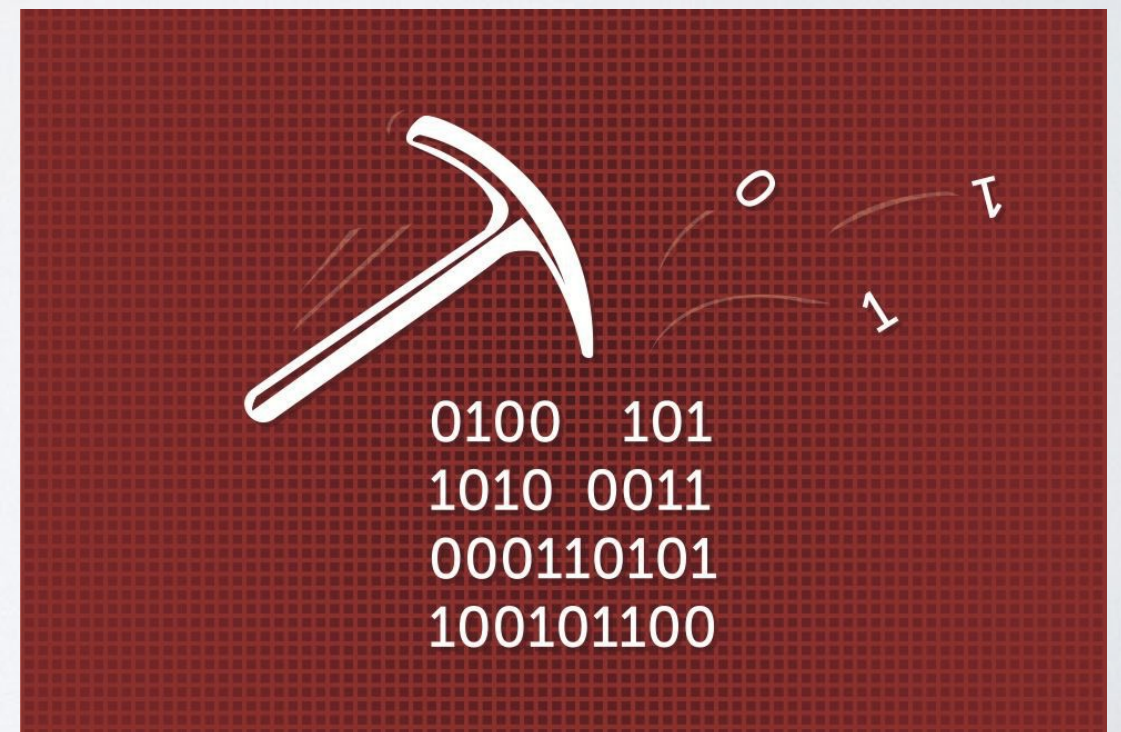
Bányászat

Bányászat

A bányászok feladata jóváhagyni és ellenőrizni a tranzakciókat, illetve új blokkokat létrehozni.

Típusok:

- GPU
- ASIC
- Felhő alapú (cloud)



Bányászat

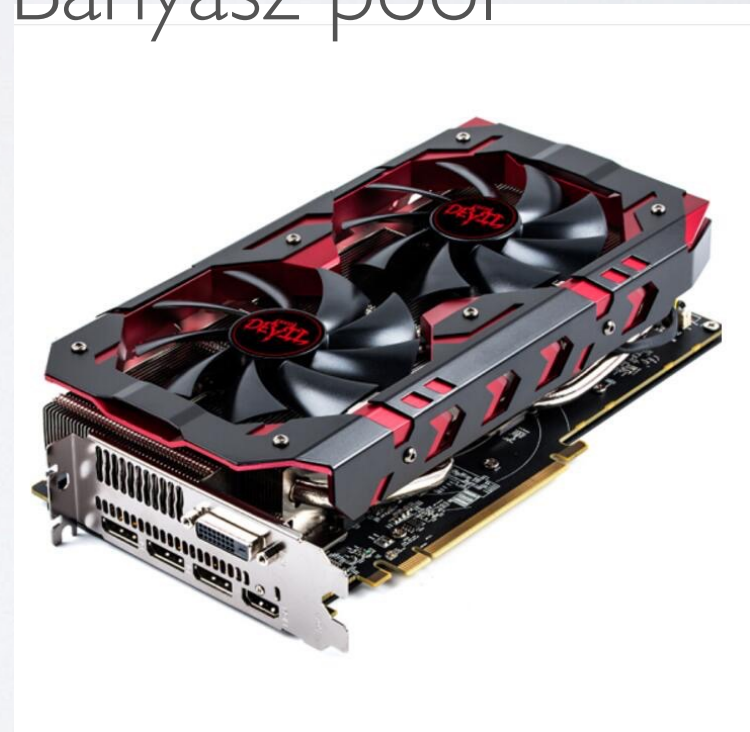
ASIC

- Célhardver
- Internet hozzáférés
- Pénztárca
- Bányász pool



GPU

- Speciális asztali PC
- Videó kártyák
- Internet hozzáférés
- Pénztárca
- Bányász pool



Bányászat

ASIC

- Könnyű, gyors konfiguráció
- 1 támogatott kriptovaluta
- Nehezebb javítani
- Kizárólag bányászatra használható
- Magas meghibásodási arány

GPU

- Minimális szakértelmet igényel
- Könnyen változtatható valuta
- Könnyű javítani
- Fejleszthető
- Másra is felhasználható

VGA bányagép



ASIC bányafarm



Bányászat

2017. december

Hashrate	13	TH/s ?
Difficulty	1347,0014	G
Block Reward:	12,5	BTC
BTC Price	10000	USD ?
Power	1200	W ?
Power Cost	0,14	USD / kWh
Pool Fee	1	%
Reject Rate:	1	%
Diff Change	-105,84	G / Month ?
Live Stats	☐ Off	

Profits At This Difficulty

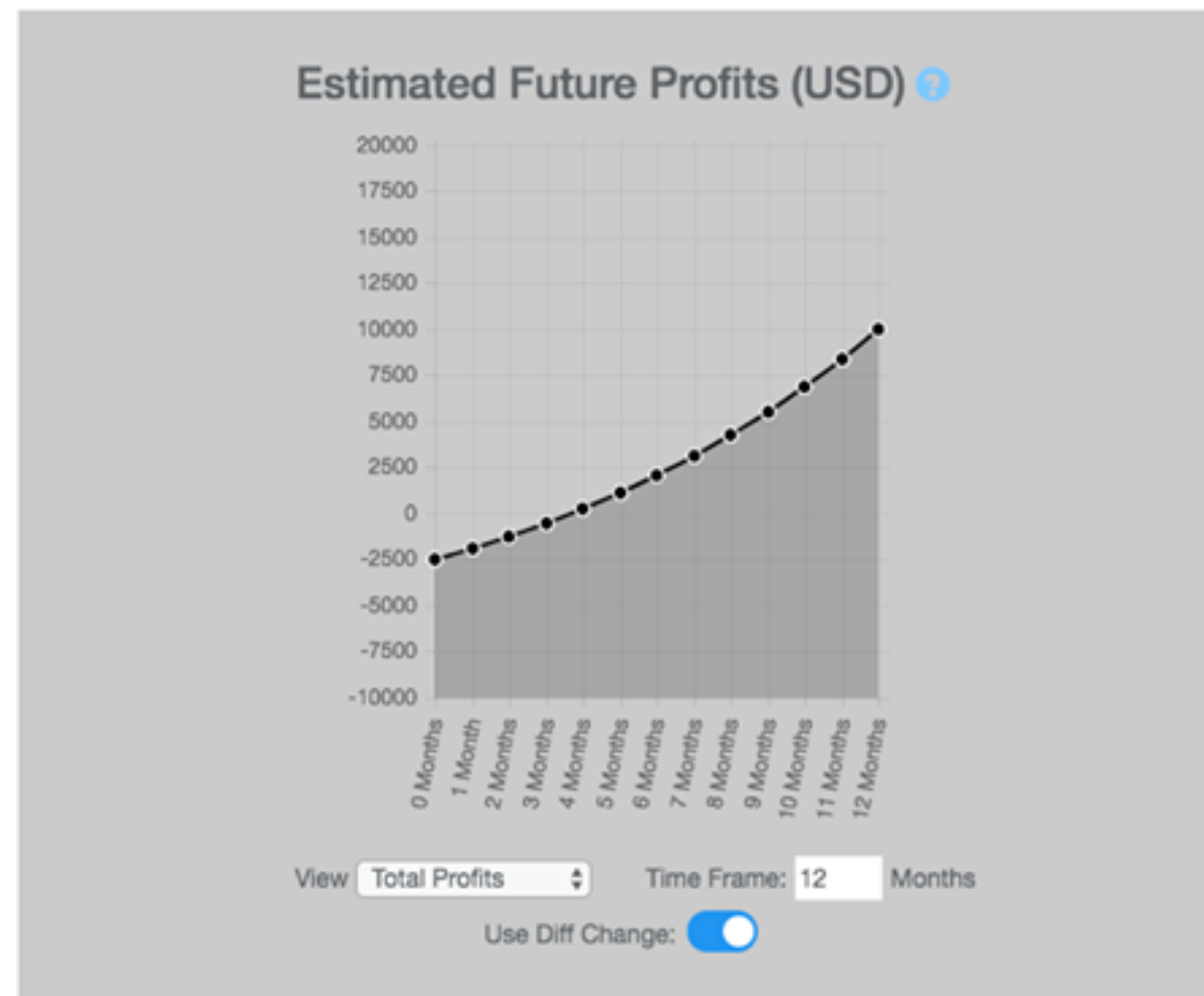
Period	BTC	USD	Costs (USD)	Profit (USD)
Hourly	0.00	\$0.991	\$0.168	\$0.823
Daily	0.00	\$23.78	\$4.03	\$19.75
Weekly	0.0166	\$166.48	\$28.22	\$138.26
Monthly	0.0713	\$713.49	\$120.96	\$592.53

Break-Even Analysis

Profitable in 3 Months 3 Weeks ?

Hardware Cost	2500	USD ?
Recurring Costs	0	USD / Month ?
Use Diff Change	☒	

Bitcoin Mining Calculator



Forrás: www.mycryptobuddy.com/BitcoinMiningCalculator

Bányászat

2018. április

Bitcoin Mining Calculator

Hashrate	14	TH/s
Difficulty	3511,0606	G
Block Reward:	12,5	BTC
BTC Price	7362,12	USD
Power	1200	W
Power Cost	0,14	USD / kWh
Pool Fee	1	%
Reject Rate:	1	%
Live Stats	☒ On	

Profits At This Difficulty

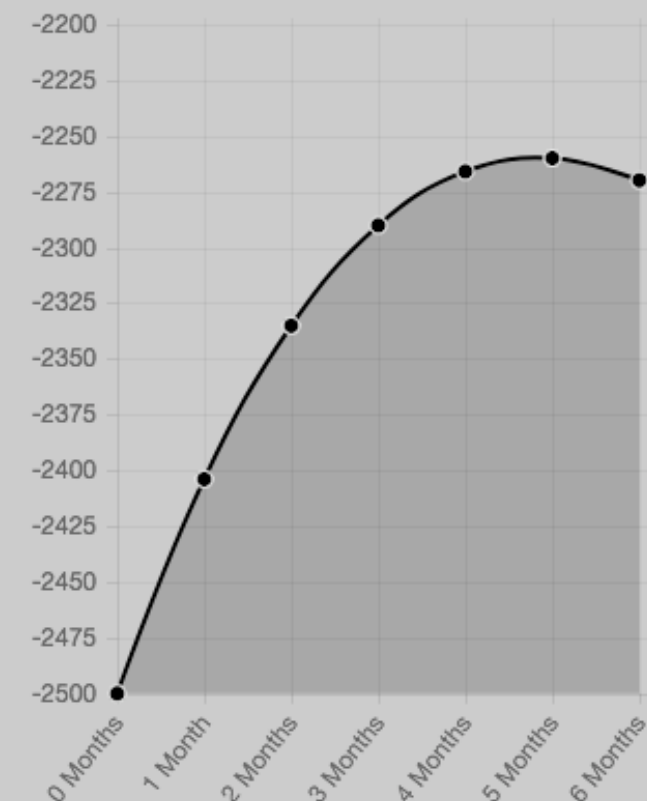
Period	BTC	USD	Costs (USD)	Profit (USD)
Hourly	0.0000409	\$0.301	\$0.168	\$0.133
Daily	0.000983	\$7.23	\$4.03	\$3.20
Weekly	0.00688	\$50.64	\$28.22	\$22.41
Monthly	0.0295	\$217.02	\$120.96	\$96.06

Long-Term Projections

Profitable in Never

Hardware Cost	2500	USD
Recurring Costs	0	USD / Month
Price Change	0	% / Month
Selling Profile	Sell Coins Monthly	
Diff Change	14,35	% / Month
Use Diff Change	☒	

Estimated Future Profits (USD)



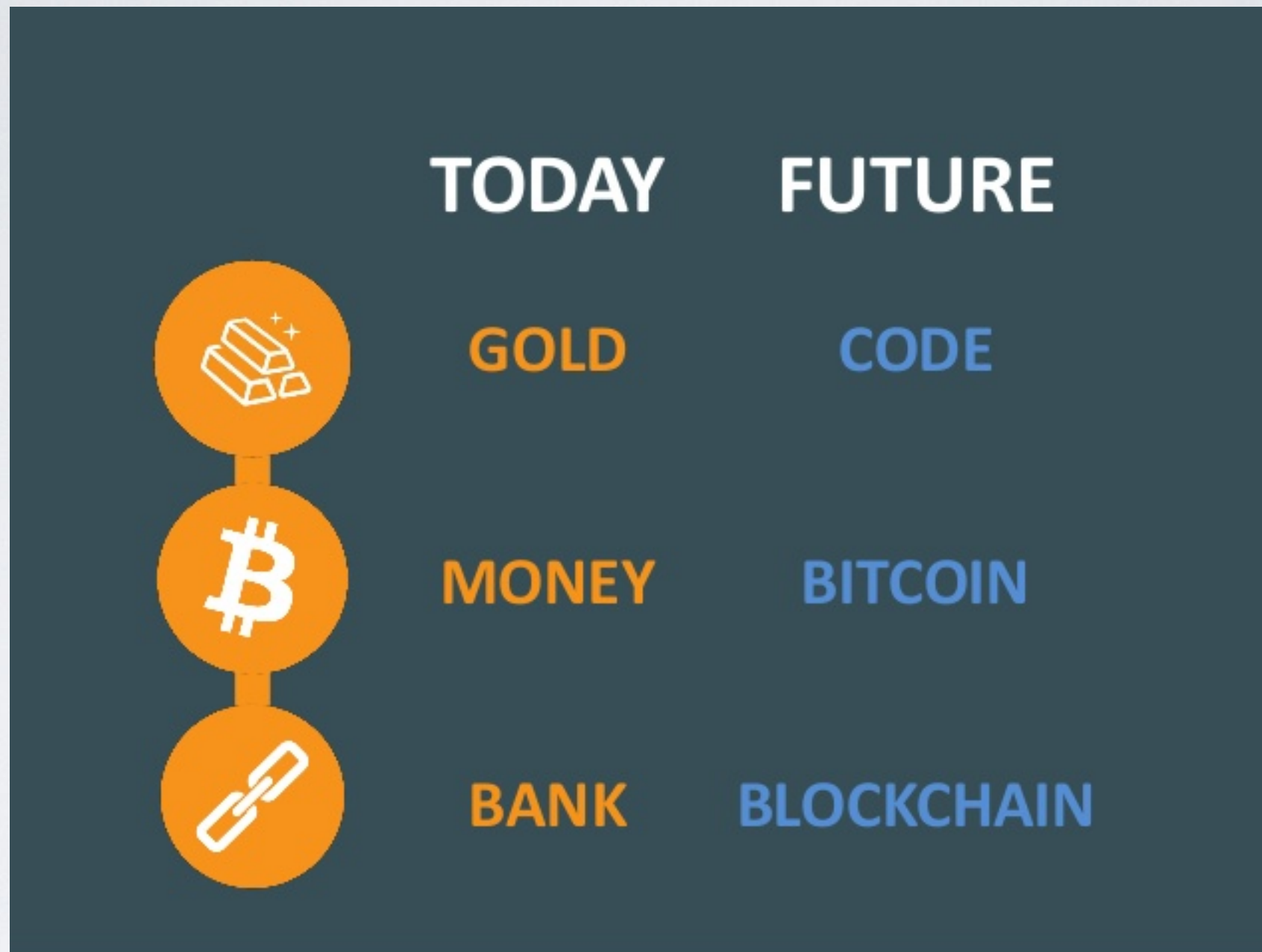
View: Total Profits Time Frame: 6 Months

Use Diff Change: ☒

Forrás: www.mycryptobuddy.com/BitcoinMiningCalculator

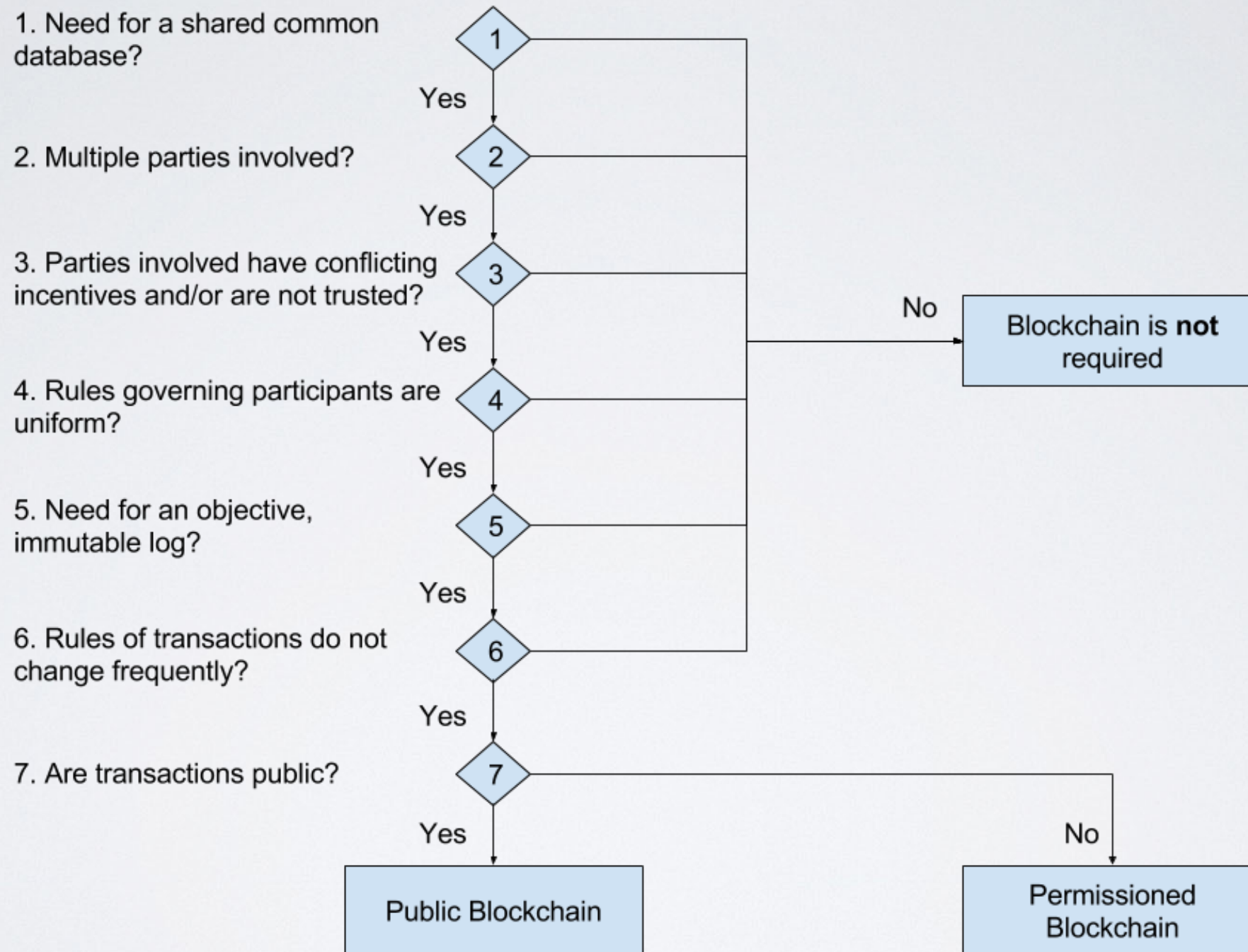
Jövő...

Jövő?



Jövő?

Blockchain Decision Path



Jövő?

Mágváltoztathatatlan naplófájl

- *Log File Authentication and Storage on Blockchain Network*
 - Publikáció: <https://ieeexplore.ieee.org/document/8524848>
 - Sándor Barnabás, Fehér Dávid János
-
- Az első és második generációs blokklánc rendszerek egyik legfontosabb tulajdonsága a megváltoztathatatlanság. Ha egy tranzakció vagy adat bekerül a láncba, akkor az örökre ott is marad. Ennek legfőbb oka az, hogy a kritikus adatokat garantáltan ne lehessen manipulálni.

Kérdések & Válaszok

Köszönöm a figyelmet!

Sándor Barnabás

sandor.barnabas@gmail.com



KELETI KÁROLY
GAZDASÁGI KAR



Jánossy Ferenc Szakkollégium



Nagyobb rálátás a világra!