Bitmono

Ĉu daŭripova mono ?

Marco van Hulten

4a de junio 2022

Enhavo

1. Enkonduko
2. Sekureco
3. Ekonomio
4. Retoriko
5. Konkludo

Kio estas Bitmono esence ?

Bitmono estas

- virtuala mono
- kies kaslibro estas malcentralizita.

Kio estas Bitmono esence ?

Bitmono estas

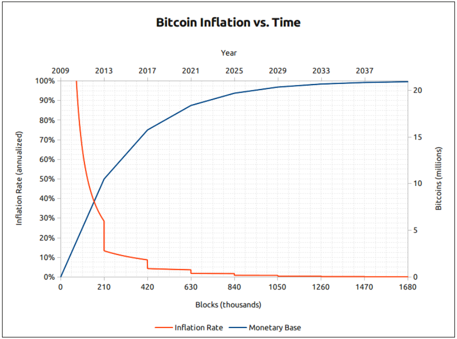
- virtuala mono
- kies kaslibro estas malcentralizita.

Pli precize, la kaslibro estas datumbazo konsistanta el « blokoj », kolektoj de datumoj. Alivorte, ĉiuj interkonsentitaj blokoj formas la kaslibron—nomitan « blokĉeno ».

Kio estas Bitmono praktike ?

Ecoj de Bitmono :

- Moneca
  - Interŝanĝo
  - Kalkulo
  - Valoro
- Limigita
- Malcentralizita
  - Aŭtonomio
  - Demokratio
  - Neniu cenzuro
- Sekura
- Libera



Libera programaro

Libera programo estas programo kiu donas al la uzanto

- La liberecon ruli la programon, por iu ajn celo
- La liberecon studi kiel la programo funkcias kaj ĝustigi ĝin laŭdezire
- La liberecon disdoni kopiojn de la programo por helpi viajn kunulojn
- La liberecon plibonigi la programon kaj publikigi viajn plibonigojn por la profito de la tuta komunumo

Ĝi gravas

- por Bitmono ĉar ĝi montras kiel la mono funkcias—ĝi estas malkaŝa
- ĝenerale ĉar el ĝi rezultas daŭripova evoluo de programaro kaj aparatoj

Kiel funkcias Bitmono

La transakcioj :

1. Krei transakcion
2. Elsendi transakcion al la Bitmono-reto
3. Ĉu valida? ⟶ Stokita en la duma transakcia stokejo (« mempool »)

La minado :

1. Ministo agregas stokitajn transakciojn en kandidatan blokon
2. La ministo provas solvi matematikan problemon
3. Se ri trovas solvon, bloko estas aldonita al la blokĉeno
4. Alia ministo verŝajne minados la sekvantan blokon sur la antaŭa
5. ...

La ministoj estas stimulataj per la bloka premio (monkreado) kaj la transakciaj kostoj.

Historio

	1983	Blindaj subskriboj de David Chaum
	1997/2002	Hashcash de Adam Back
฿	2008	Cifereca monosistemo de Satoshi Nakamoto
฿	2009	Genezobloko elfosita
ɱ	2014	« Monero » (ringsubskriboj, anonima)
Ξ	2015	« Ethereum » (aplikaĵoplatformo)
฿	2017	Aktivigo de apartiga atesto (« SegWit »)
฿	2019	Unua kondukata pagreto (« Lightning »)
฿	2021	Pli disa uzo de Lightning en Salvadoro
฿	2021	« Taproot » $\longrightarrow$ pli da privateco, inteligentaj kontraktoj, ...
฿	2022	Rusio adoptas Bitmonon (komerco kaj minado)

Teorie

- Malcentra konsentmeĥanismo
- Pruvo de laboro (PoW)
- SHA-256
- Publikŝlosila ĉifro por transakcioj
- Tamen 51 %-atako (eble)
- Nelineare fortaj komputiloj, ekz. kvantumkomputiloj

Kvantuma komputilo

Kvantumsekura ?

- Praktika kvantuma komputilo povus krevigi SHA-256
  - Nenuna zorgo, sed ŝanĝi kriptologion de blokĉeno ne trivialas
  - La tuta mondo uzas SHA-256
- Publika ŝlosilo facile kodrompita
  - Ĉiam sendi al nova adreso
    - Tamen ekzistas limhava tempo dum kiu transakcio estas en la duma transakcia stokejo
  - Alternativo : NTRU (krada kriptologio, rezista kontraŭ la Shor-algoritmo)

Praktike

Ĝenerale fortika, sed

- aŭgusto 2010 — Bloko 74 638 enhavis transakcion kiu kreis pli ol 184 miljardojn da bitmono
- marto 2013 — Versio 0.8 nekongrua (forgesita bloklimo)

Praktike

Ĝenerale fortika, sed

aŭgusto 2010 Bloko 74 638 enhavis transakcion kiu kreis pli ol 184 miljardojn da bitmono

marto 2013 Versio 0.8 nekongrua (forgesita bloklimo)

- Tamen neniam okazis vera disrompo de la blokĉeno.
- Ni ne parolas pri enŝteliĝo en centrajn monborsojn —konservu vian propran bitmonon !
- Ni ne parolas pri altcoins (alternativaj ciferecaj valutoj).

Nedaŭripova ekonomio

Nuntempa situacio :

- Kreado de mono
    - centra kreado de bazmono
    - bankumado kun frakciaj rezervoj

Nedaŭripova ekonomio

Nuntempa situacio :

- Kreado de mono
  - centra kreado de bazmono
  - bankumado kun frakciaj rezervoj

$\longrightarrow$

- Nedaŭra valoro de mono

Nedaŭripova ekonomio

Nuntempa situacio :

- Kreado de mono
  - centra kreado de bazmono
  - bankumado kun frakciaj rezervoj

$\longrightarrow$

- Nedaŭra valoro de mono
- Fia stimulo de konsumismo
  - Varoj kaj servoj neesencaj
  - Malŝparo, elĵetado, poluado
- Nepageblaj domoj
- Milito

Evoluo de Bitmono

- Kreskas uzo de Bitmono

Evoluo de Bitmono

- Kreskas uzo de Bitmono
- ... tamen kiel ?

Evoluo de Bitmono

- Kreskas uzo de Bitmono
- ... tamen kiel ?

Scenaroj :

1. Bitmono malaperos
2. Bitmono ekzistos plu sed neniam atingos grandan akcepton
3. Bitmono estos la unua/preferata mono

Evoluo de Bitmono : scenaro 1

La malapero de la uzo de Bitmono povus okazi se

- La valoro iros al 0 (merkato)
- Sekureco rompiĝos
- Leĝo tutmonda malpermesos la uzon aŭ minadon

Evoluo de Bitmono : scenaro 1

La malapero de la uzo de Bitmono povus okazi se

- La valoro iros al 0 (merkato)
- Sekureco rompiĝos
- Leĝo tutmonda malpermesos la uzon aŭ minadon

⟶

- Neniu uzo de energio de minado
- Trokonsumado daŭros (se nenio alia ŝanĝiĝos)
- ...

Evoluo de Bitmono : scenaro 1

La malapero de la uzo de Bitmono povus okazi se

- La valoro iros al 0 (merkato)
- Sekureco rompiĝos
- Leĝo tutmonda malpermesos la uzon aŭ minadon

⟶

- Neniu uzo de energio de minado
- Trokonsumado daŭros (se nenio alia ŝanĝiĝos)
- ...

Tamen ĉi tiu scenaro estas tre neverŝajna !

Evoluo de Bitmono : scenaro 2

Bitmono neniam atingos grandan akcepton

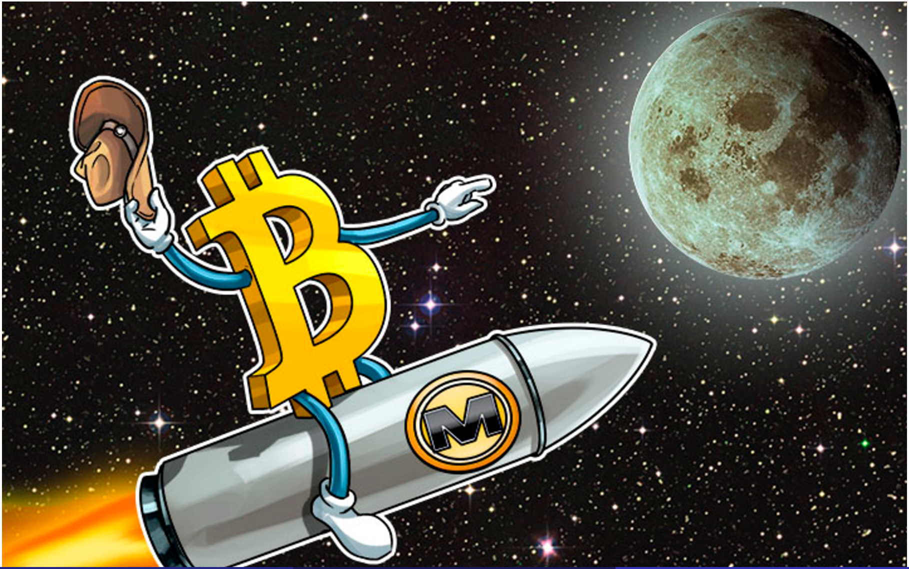
Evoluo de Bitmono : scenaro 2

Bitmono neniam atingos grandan akcepton

⟶

- Malgranda parto de la mondo profitos per la deflacia mono
- Trokonsumado, speciale de nebitmonuloj, daŭros
- Malriĉeco daŭros
- Tamen povas ekzisti interesaj aplikaĵoj
- Energiuzo de minado daŭros (pli-malpli difinita de la merkato)

Evoluo de Bitmono : scenaro 3



Evoluo de Bitmono : scenaro 3

Bitmono iĝas la unua/preferata mono

Evoluo de Bitmono : scenaro 3

Bitmono iĝas la unua/preferata mono

⟶

- La valoro estos daŭra (aŭ eĉ malinflacia)
- Homoj pli ŝparos kaj malpli konsumos
- Energiuzo de minado daŭras (pli-malpli difinita de la merkato)

Evoluo de Bitmono : scenaro 3

Bitmono iĝas la unua/preferata mono

⟶

- La valoro estos daŭra (aŭ eĉ malinflacia)
- Homoj pli ŝparos kaj malpli konsumos
- Energiuzo de minado daŭras (pli-malpli difinita de la merkato)

Ĉu la medio malpli detruiĝos ?

- Nur se la kvanto da elĵeto (« emission intensity ») de minado signife malkreskas

Ĉu transakcioj kostas multe da energio ?

- Principe praktike nulo
- Aprezo de ₿ $\longrightarrow$ pli da minado
  - Minado certigas la Bitmono-reton
- Transakcioj stokiĝas en blokon kaj sur la blokĉeno
  - Transakci-kompenso (tx fees)
  - Eble tiu kompenso tradukiĝas al energiuzo
  - Nuntempe tiuj kompensoj estas po ĉ. 1–5 USD (tamen komparu kun Lightning-reto) por transakcio
- Tamen : uzo de la sistemo ; komparu la interdependecon inter nafto kaj aproba mono (« fiat »)

Energikomparo

La homaro uzas 167 705 TW h jare.

Bitmono uzas[1]

- 120 TW h jare
- 85 % de la norvega popolo
- 0,55 % de la elektrouzo de la homaro
- 0,19 % de la konstruindustrio
- 0,07 % de la energiuzo de la homaro

[1] Datumoj venas de diversaj fontoj de aŭg. 2021 ĝis majo 2022.

Energikomparo

La homaro uzas 167 705 TW h jare.

Bitmono uzas[1]

- 120 TW h jare
- 85 % de la norvega popolo
- 0,55 % de la elektrouzo de la homaro
- 0,19 % de la konstruindustrio
- 0,07 % de la energiuzo de la homaro

kaj elpuŝas

- 22 Mt de CO_2
- 0,18 % de la konstruindustrio
- 0,28 % de la transportindustrio
- 1,6 % de la financo- kaj asekuro-industrio

[1] Datumoj venas de diversaj fontoj de aŭg. 2021 ĝis majo 2022.

Anonimeco kaj malbona uzo

1. Anonimeco estas kondiĉo por libereco
2. Ni bezonas anoniman pagmanieron
3. Bitmono ne estas anonima (originale)

Anonimeco kaj malbona uzo

1. Anonimeco estas kondiĉo por libereco
2. Ni bezonas anoniman pagmanieron
3. Bitmono ne estas anonima (originale)

Kio pri krimuloj ?

- Bitmono estas relative maltaŭga por fiaĵoj
- La aproba sistemo estas uzata por tio, ĉu kontanto ĉu iuj « legitimaj » financaj priservoj
- La plejmulto de fiagoj lasas spurojn, eble kaj sur la blokĉeno, kaj en la fizika mondo

Deirpunkto

Se vi kredas ke Bitmono ne havas valoron apriore, se vi ne vidas ke ĝi povus havi valoron por socio, ĉiu ajn energiouzo, ĉiu ajn kriminaleco, ĉiu ajn malgajno estu rigardata kiel kialo ke Bitmono ne ekzistu. Oni devus pensi kiel ĉesigi Bitmonon, ekzemple malpermesante minadon. Tamen tio estos preskaŭ neebla. Imagu :

1. Multaj naciaj registaroj malpermesas minadon
2. La malfacileco de minado malpliiĝas
3. La financa instigo de minado kreskas
4. Aliaj landoj minados bitmonon

Tutmonda malpermeso

Imagu ke vi havas mondregistaro kiu

1. malpermesas minadon tutmonde
2. $\longrightarrow$ La malfacileco de minado malpliiĝas (teorie al nulo)
3. $\longrightarrow$ Iu povus sekrete elfosi bitmonon kun granda sukceso

Tutmonda malpermeso

Imagu ke vi havas mondregistaro kiu

1. malpermesas minadon tutmonde
2. ⟶ La malfacileco de minado malpliiĝas (teorie al nulo)
3. ⟶ Iu povus sekrete elfosi bitmonon kun granda sukceso

Ju pli da minado estas malpermesata, des pli da inklino al minado.

Minado kun renovigebla energio

Se vi akceptas la pluekzistadon de Bitmono, pli da minado kun renovigebla energio havas pozitivan efikon sur la medion. Imagu ke la Bitmono-reto klinas al konstanta haketa povumo, kaj (pro tio) iu komencas minadon.

- $\longrightarrow$ Pli da haketa povumo estas aldonita
- $\longrightarrow$ Malfacileco kreskas
- $\longrightarrow$ Malpli da inklino al minado do tutmonde malpli da minado

Minado kun renovigebla energio

Se vi akceptas la pluekzistadon de Bitmono, pli da minado kun renovigebla energio havas pozitivan efikon sur la medion. Imagu ke la Bitmono-reto klinas al konstanta haketa povumo, kaj (pro tio) iu komencas minadon.

- ⟶ Pli da haketa povumo estas aldonita
- ⟶ Malfacileco kreskas
- ⟶ Malpli da inklino al minado do tutmonde malpli da minado

Sekvas ke se tiu aldonita haketa povumo estas renovigebla energio, ke post malfacileco-ŝanĝo la parto de renovigebla minado kreskas.

Ekzemploj : vulkana varmego (Salvadoro), akva energio (Norvegio)

Minado kun troaĵo da energio

- Renovigebla
- Nuklea energio

Se oni akceptas la ekziston de Bitmono, oni devus stimuli la minadon per renovigebla kaj troaĵa energio.

Konkludoj

- Bitmono estas kreita kiel respondo al problemoj kun la mona kaj financa sistemoj
- Bitmono estas necentraliza, do iu ajn povas uzi ĝin kaj estas malfacila prohibi ĝin

Konkludoj

- Bitmono estas kreita kiel respondo al problemoj kun la mona kaj financa sistemoj
- Bitmono estas necentraliza, do iu ajn povas uzi ĝin kaj estas malfacila prohibi ĝin

Bitmono havas pozitivajn kaj negativajn ecojn

- Ekonomie kaj demokrate Bitmono eble bonas
    - Potenco de ŝparema livstilo

Konkludoj

- Bitmono estas kreita kiel respondo al problemoj kun la mona kaj financa sistemoj
- Bitmono estas necentraliza, do iu ajn povas uzi ĝin kaj estas malfacila prohibi ĝin

Bitmono havas pozitivajn kaj negativajn ecojn

- Ekonomie kaj demokrate Bitmono eble bonas
    - Potenco de ŝparema livstilo
- La minado kostas energion definitan de la merkato
- La minado bezonas mineralojn (ASIC-komputiloj)

Konkludoj

- Bitmono estas kreita kiel respondo al problemoj kun la mona kaj financa sistemoj
- Bitmono estas necentraliza, do iu ajn povas uzi ĝin kaj estas malfacila prohibi ĝin

Bitmono havas pozitivajn kaj negativajn ecojn

- Ekonomie kaj demokrate Bitmono eble bonas
  - Potenco de ŝparema livstilo

- La minado kostas energion definitan de la merkato
- La minado bezonas mineralojn (ASIC-komputiloj)

- Tamen kiom kostas la nuna sistemo de aproba mono ?

Bitcoin energy use vs. other industries.
https://bitcoinmagazine.com/business/bitcoin-energy-use-compare-industry.

Russia will eventually legalize Bitcoin.
https://bitcoinmagazine.com/markets/russia-will-eventually-legalize-bitcoin.

Akcora, C. G., Gel, Y. R., and Kantarcioglu, M. (2022).
Blockchain networks: Data structures of bitcoin, monero, zcash, ethereum, ripple, and iota.
WIREs Data Mining and Knowledge Discovery, 12(1):e1436.

Antonopoulos, A. M. (2017).
Mastering Bitcoin.

Bernstein, D., Chuengsatiansup, C., Lange, T., and van Vredendaal, C. (2016).
NTRU Prime.

Chaum, D. (1983).
Blind signatures for untraceable payments.
In Chaum, D., Rivest, R. L., and Sherman, A. T., editors, Advances in Cryptology, pages 199–203, Boston, MA. Springer US.

Nakamoto, S. (2008).
Bitcoin: A Peer-to-Peer Electronic Cash System.

Stallman, R. (2012).
The free software definition.

Swan, G.
Bitcoin Canon.
https://www.swanbitcoin.com/canon.

Aplikaĵoj

« Bitcoin Core » estas la referencrealigo kun funkcioj kiel :

- Baza mono (tavolo 1)
- Pagkanaloj, ekz. « Lightning »
    - Rapidaj kaj granulaj pagoj
    - Pli granda privateco
    - Atomaj komutoj
- « Counterparty »
    - Inteligentaj kontraktoj (DeFi, DAO)
    - Neinterŝanĝeblaj ĵetonoj (NFT)
- Malcentralizaj identecoj

Kiel funkcias la Lightning-reton ?

Pagadreto : senfida interŝanĝo de Bitmono el la blokĉeno

1. Monkolektado (ankrotransakcio) kiu fiksas la komunuman staton sur la blokĉeno
2. Interkonsento-transakcioj el-ĉenaj
3. Kvitiĝo-transakcio sur la blokĉeno

Internaciaj valutoj

simbolo	esperante	angle	priskribo
Spesmilo-simbolo, Sm	spesmilo	spesmilo	nekutima fizika mono (1907–1914)
★	stelo	stelo	esperanta mono (1942–??)
₿, BTC	bitmono	bitcoin	la originala kriptovaluto (2009–)
sat	satoŝi	satoshi	10^{-8} ₿
ɱ, XMR	monero	monero	privata ĉifromono (2014–)
Ξ, ETH	etero	ether	alia kriptovaluto (2015–)

Internaciaj valutoj

Rilate la 17 Celojn por Daŭripovan Evoluigon

La sekvaj potencialaj efikoj temas nur pri la moneco de Bitmono; ekzistas aliaj aplikaĵoj (inteligentaj kontraktoj).

Celo	Pozitiva	Negativa
1 : Neniu malriĉo	Ne bezonas bankkonton	Riĉodistribuo
4 : Bonkvalita edukado	Edukado pri ekonomio	–
7 : Pagebla kaj pura energio	Nova infrastrukturo	Bezonas energion
8 : Bona laboro kaj ekonomia kresko	Pli racia kresko	Spekulacio
9 : Industrio, inventemo, infrastrukturo	Nova industrio k.t.p.	–
10 : Redukti malegalecon	Mono por ĉiu	Riĉodistribuo
12 : Respondecaj konsumo kaj produkto	Bitmonuloj ŝparas ?	Konstruo de komputilo
13 : Klimata agado	–	Bezonas energion
16 : Paco, justo, fortaj institucioj	Demokrata institucio	Neŭtrala pri paco/justo