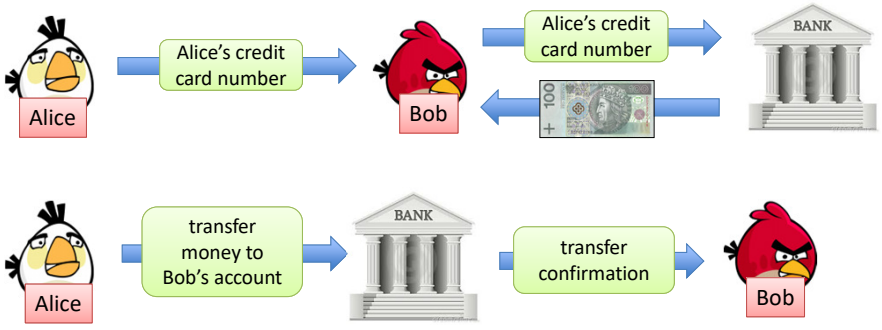
Curs ASI

1

Metode de plată digitale "clasice"



PROBLEME

1.server centralizat („bancă") necesar pentru fiecare tranzacție
2. comisioane per tranzacție
3. lipsa anonimității

2

Monedă digitală autentică

Bitcoin!

Creată de "Satoshi Nakamoto" în 2008-2009

(persoană sau grup de persoane; a rămas necunoscut și a "dispărut" în 2010 după ce a definit conceptul și a publicat software-ul Bitcoin-QT)

unitate: **Bitcoin (BTC)**.

subdiviziune: **1 BTC = 10^8 Satoshi**

se folosește și **milibitcoin (mBTC)**

3

Bitcoin

în Bitcoin:

fără server central

comisioane mici

"pseudo-anonimitate"

Problemele precedente

1. server central
2. comisioane mari
3. lipsa anonimității

4

"Fără server central"

Nu există control centralizat al monedei:

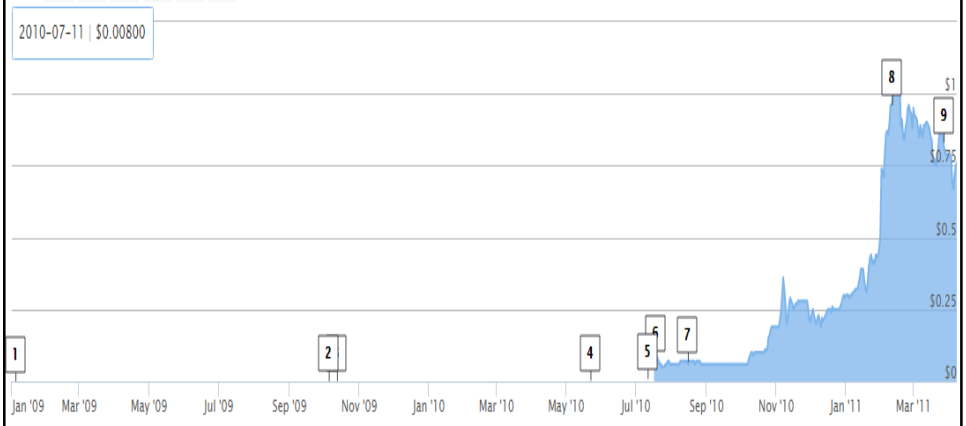
- Suma totală aflată în circulație crește de la 0 la o sumă maximă teoretică de 21 milioane BTC → **fără inflație**
- **rata de schimb variază puternic**
- lipsa serverului central compensată în mod ingenios printr-un protocol care face ca un grup mare de useri să prevină tehnic (computațional) posibilele fraude comise de un grup mic de useri.

5

Istoric, p.1

La origine (3 ian 2009): 1BTC = 0.0009 $

feb 2011: 1BTC = 1 $



sursa: *https://bitcoinhelp.net/know/more/price-chart-history* pt. semnificația cifrelor [1], [2] (evenimente care au influențat valoarea Bitcoin)

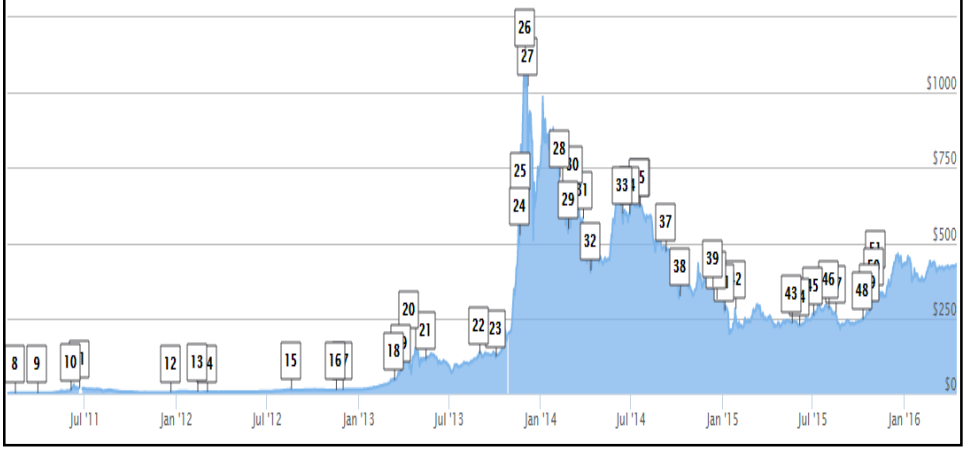
6

Istoric, p.2

noiembrie 2013: 1BTC = 1242 $

iulie 2015: 1BTC = 226 $

aprilie 2016: 1BTC = 430 $



7

Istoric, p.3

februarie 2017: 1BTC = 1000 $

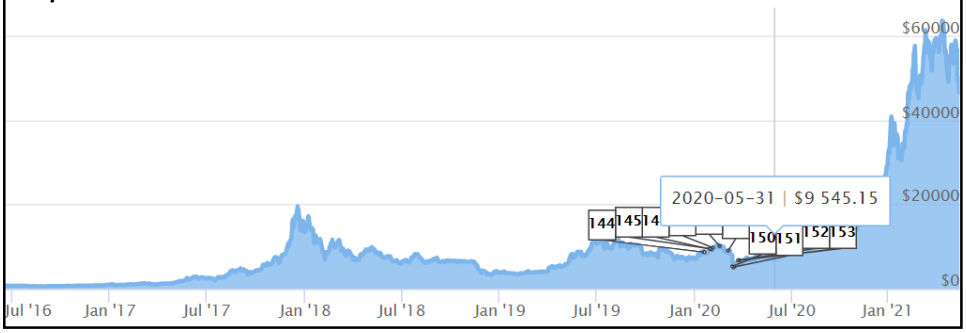
decembrie 2017: 1BTC = 19500 $

februarie 2018: 1BTC = 6800 $

decembrie 2018: 1BTC= 3000$

ianuarie 2021: 1BTC=40000$

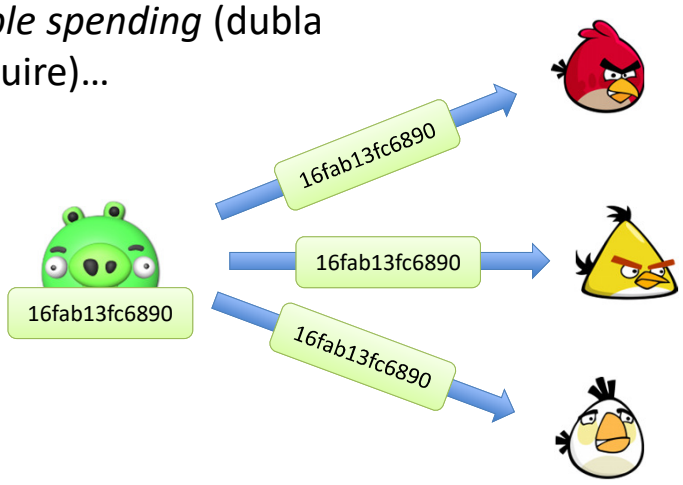
aprilie 2021: 1BTC=63000$



8

Principala problemă a monedelor digitale

Double spending (dubla cheltuire)…



Biții se copiază mai ușor decît bancnotele!

9

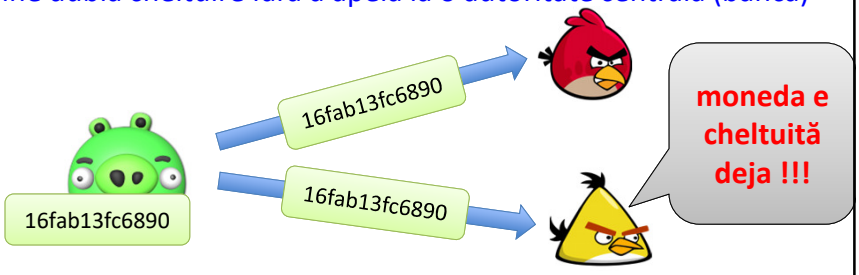
Principiul Bitcoin

Utilizatorii simulează listarea tuturor tranzacțiilor la un "avizier" public, implementat sub forma unei rețele P2P.

Exemplu de tranzacție:

"User P_1 transferă moneda #16fab13fc6890 către user P_2"

Se previne dubla cheltuire fără a apela la o autoritate centrală (banca)



10

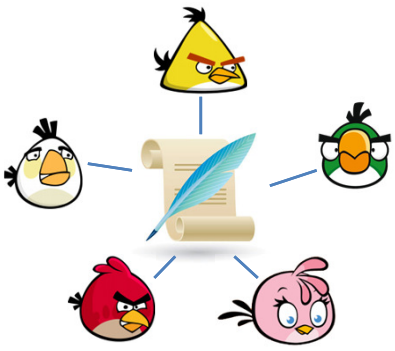
Probleme

1. Cum se implementează “avizierul” ?
2. Cum se identifică utilizatorii?
3. De unde provin banii?
4. Care e sintaxa tranzacțiilor?

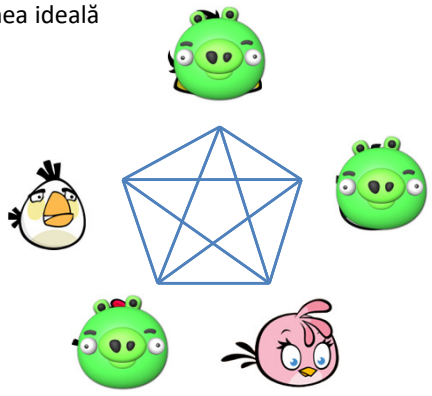
11

Emularea “avizierului”

lumea ideală



protocol într-o rețea P2P care emulează lumea ideală



Problema principală: Unii participanți pot trișa.

Rezultat clasic: sistemul funcționează dacă majoritatea este cinstită.

12

Problemă

Cum definim "**majoritatea**" într-o situație în care

oricine se poate alătura rețelei?

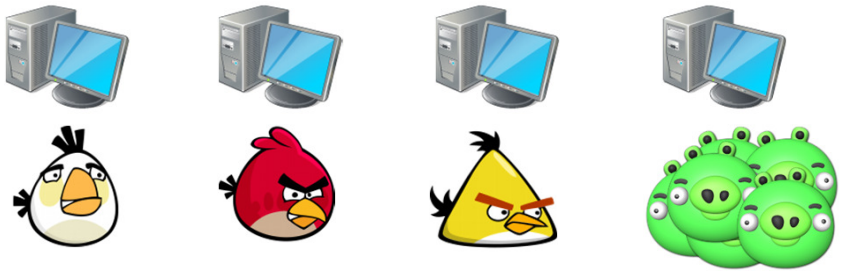
13

Soluția BitCoin

Definim "majoritatea" drept

majoritatea puterii de calcul

Deci, nu ajută să creăm identități multiple!



14

Cum se verifică?

Ideea de bază:

•utilizează **Proofs of Work (PoW)**
•**motivează** userii cinstiți să participe prin răsplătirea lor - minerii!

Userii cinstiți pot utiliza ciclii **CPU sau GPU nefolosiți** (la origine)

Dar: în momentul de față, se face folosind **hardware dedicat (și scump)**.

15

Proofs of Work (PoWs)

Introdus de **Dwork și Naor** [Crypto 1992] ca o apărare împotriva spam-ului.

ideea de bază:
Obligă userii să lucreze la o problemă computațional intensivă: rezolvă un "puzzle" de complexitate moderată, dar a cărui soluție e foarte ușor de verificat.

Un **PoW** simplu e bazat pe **funcții hash.**

16

Funcții hash

O funcție hash întoarce un rezultat care se modifică **foarte mult**, la orice **mică** modificare a input-ului

Exemple: SHA1, SHA3, RIPEMD,…

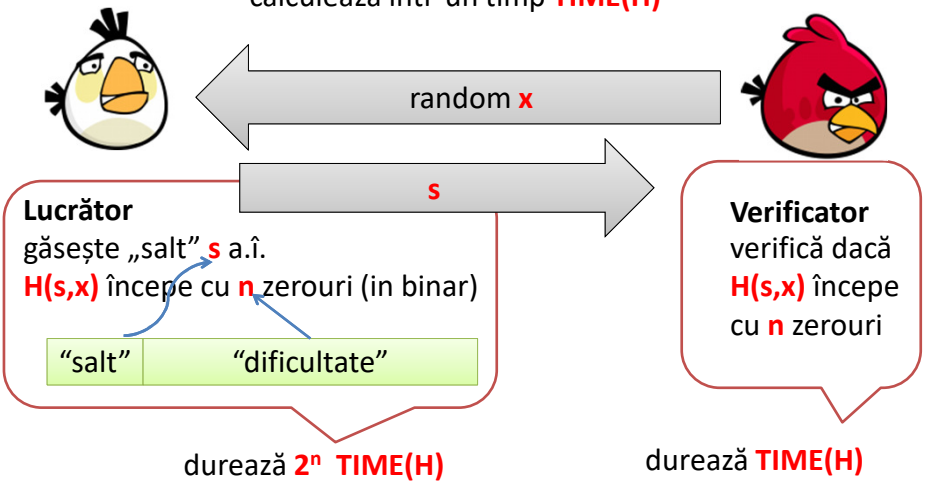
SHA1(Bedlewo) = 6533a9b2ab79e57a555bc3a7cdbc58998d6000f0
SHA1(Bendlewo) = f2a5a0cb8b942fbcb472a4cf6d6699ff6f630c71

Proprietate: singurul mod de a găsi **x** a.î. **H(x)** are anumite proprietăți este *forța brută*.

17

Utilizarea hash ca PoW

H -- o funcție hash care se calculează într-un timp **TIME(H)**

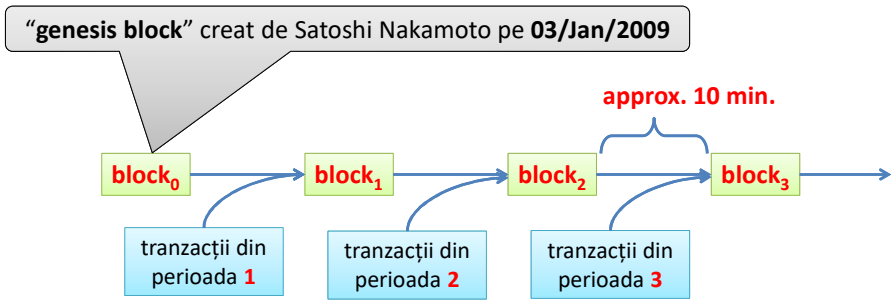


18

Ideea de bază

Participanții la schemă se numesc “mineri”.

Ei mențin un lanț de blocuri *(block chain):*



19

Cum se “publică la avizier”

1) Oricine face o tranzacție o transmite prin Internet (în mod **broadcast**) în cadrul unei **rețele P2P** în care sînt conectați minerii

2) minerii sînt motivați să lucreze asupra ei.

3)tranzacția va fi verificată și adăugată la următorul bloc.

20

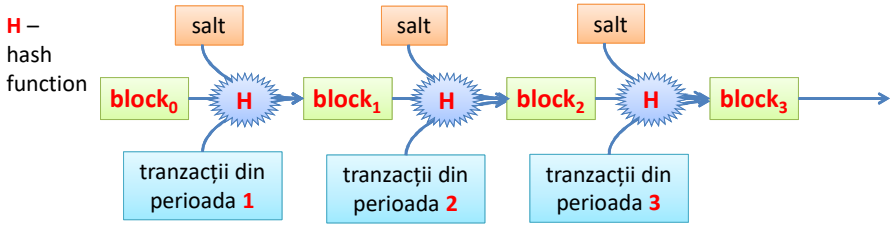
Principii de bază

1. Este **computational intensiv** să se extindă lanțul de blocuri prin găsirea unui nou bloc care să satisfacă condiția precedentă
2. Primul miner care găsește soluția problemei și găsește un nou bloc pentru a extinde lanțul, îl trimite (**broadcast) către toată lumea**
3. Userii vor accepta "**cel mai lung lanț**" drept cel valid

sistemul îi motivează financiar să o facă, prin plata în Bitcoins

21

Cum se utilizează PoWs ?



Extinderea *blockchain* se face atunci cînd un miner găsește valoarea **salt** (**Nonce** în notația lui Nakamoto) a.î.

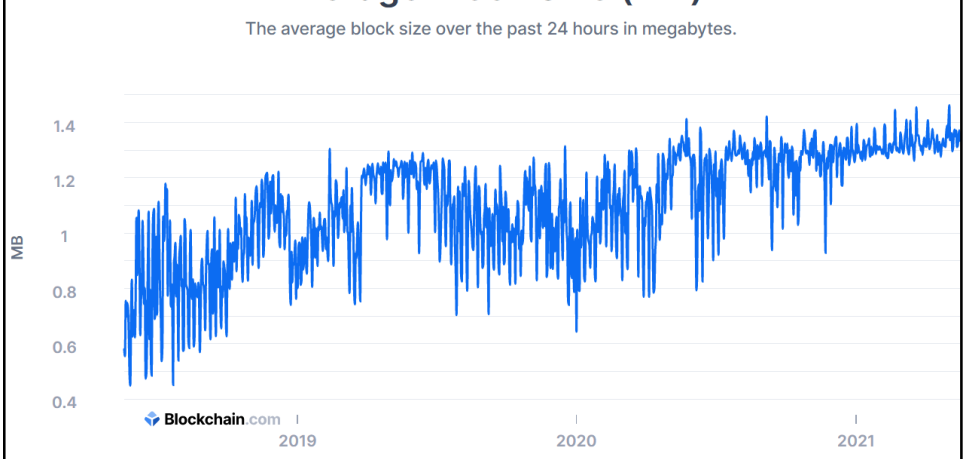
H(salt, block$_i$,transactions) începe cu **n zerouri**

sau, echivalent cu

H(salt, block$_i$,transactions) < o valoare dată

22

Ce dimensiune are un bloc?



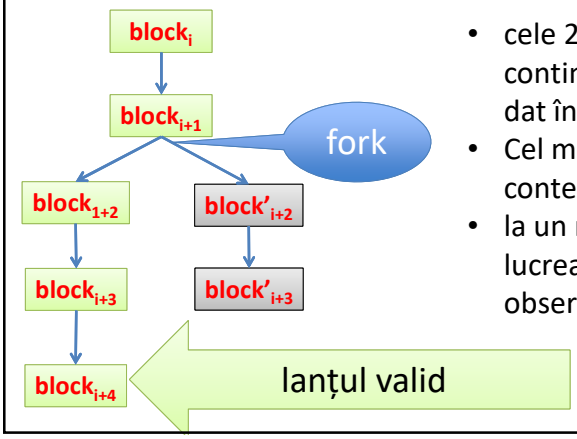
Dimensiunea unui bloc=aprox 1 -1.4 MBytes.

Dimensiunea a crescut în ultimii ani de funcționare (în 2013 un bloc avea 100-200Kbytes). Dimens. crește căci nr. de tranzacții în rețea crește.

23

Ce se întîmplă în caz de "fork"?

- doi mineri pot găsi soluția aproape în același timp, și trimit cîte un nou bloc în rețea
- datorită timpilor de propagare în rețea, în anumite noduri ale rețelei ajunge unul sau altul din cele 2 noi blocuri: $block_{i+2}$ sau $block'_{i+2}$
- se crează 2 lanțuri diferite → s.n. **fork**

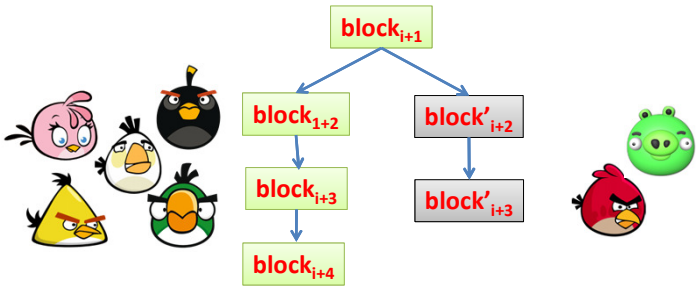


- cele 2 lanțuri care s-au creat vor continua în paralel, la un moment dat însă unul va deveni mai lung
- Cel mai **lung** lanț e cel care contează.
- la un moment dat cei care lucrează la lanțul mai scurt vor observa asta și se vor opri.

24

Are sens să se lucreze pe un lanț mai scurt?

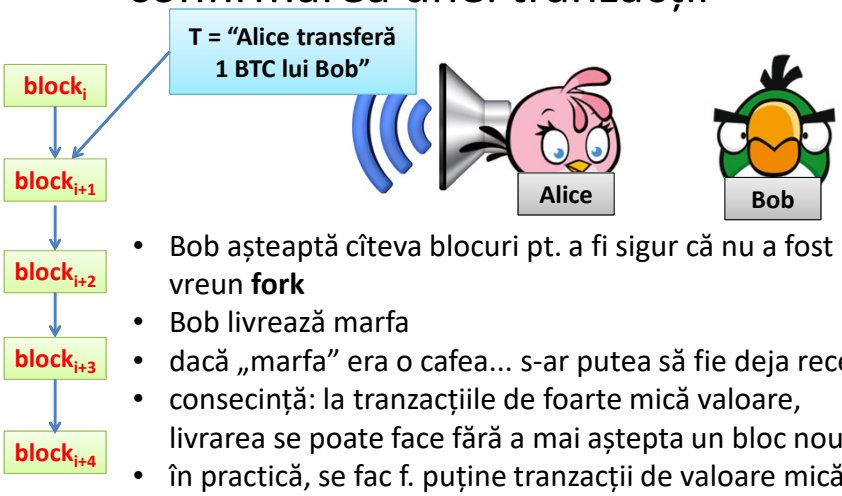
Nu!



- Pe măsură ce tot mai mulți trec să lucreze la lanțul mai lung, acesta va crește proporțional mai repede, fiind mai probabilă găsirea de noi soluții dacă sînt mai mulți mineri
- celălalt lanț va fi abandonat în scurt timp
- **Măsură de protecție:** o persoană care dorește să facă ***double spending*** ar putea **teoretic** să creeze un lanț ilicit, mai lung, care să *nu* includă tranzacția pe care vrea să o ascundă. **Practic**, în scurt timp toți ceilalți, fiind mai numeroși, vor depăși în lungime lanțul „ilicit" → aplicație ingenioasă a principiului că sistemul va funcționa corect dacă majoritatea utilizatorilor sînt cinstiți.

25

Timpul de așteptare pentru confirmarea unei tranzacții



- Bob așteaptă cîteva blocuri pt. a fi sigur că nu a fost vreun **fork**
- Bob livrează marfa
- dacă „marfa" era o cafea... s-ar putea să fie deja rece!
- consecință: la tranzacțiile de foarte mică valoare, livrarea se poate face fără a mai aștepta un bloc nou.
- în practică, se fac f. puține tranzacții de valoare mică în BTC, căci BTC nu și-a atins scopul de a fi folosit ca monedă de schimb. Este folosit în special ca investiție.

26

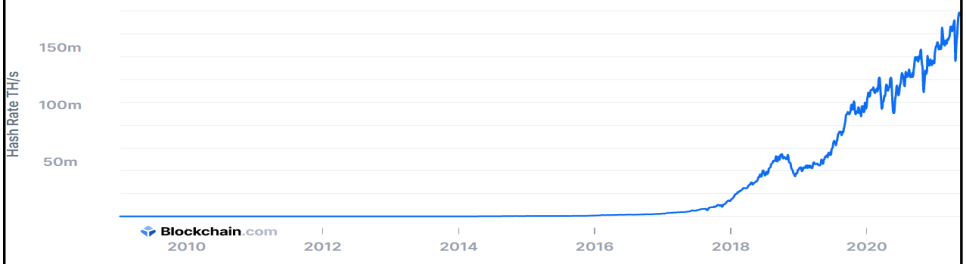
Parametrul de dificultate *n*

- *n* = nr. de biți 0 cu care să înceapă *hash*-ul
- Puterea de calcul disponibilă **crește** în timp
- Minerii trebuie să genereze un nou bloc **la fiecare 10 minute** (în medie).
- Deci, parametrul de dificultate *n* **este ajustat periodic** în funcție de performanța recentă a minerilor, a.î. timpul să rămînă cît mai aproape de 10min.
- Ajustarea se face la fiecare **2016 blocuri**
- De exemplu, blocul adăugat la 2014-03-17 18:52:10 era:

```
0000000000000006d8733e03fa9f5e5
2ec912fa82c9adfed09fbca9563cb4ce
```

27

PoW la nivel global



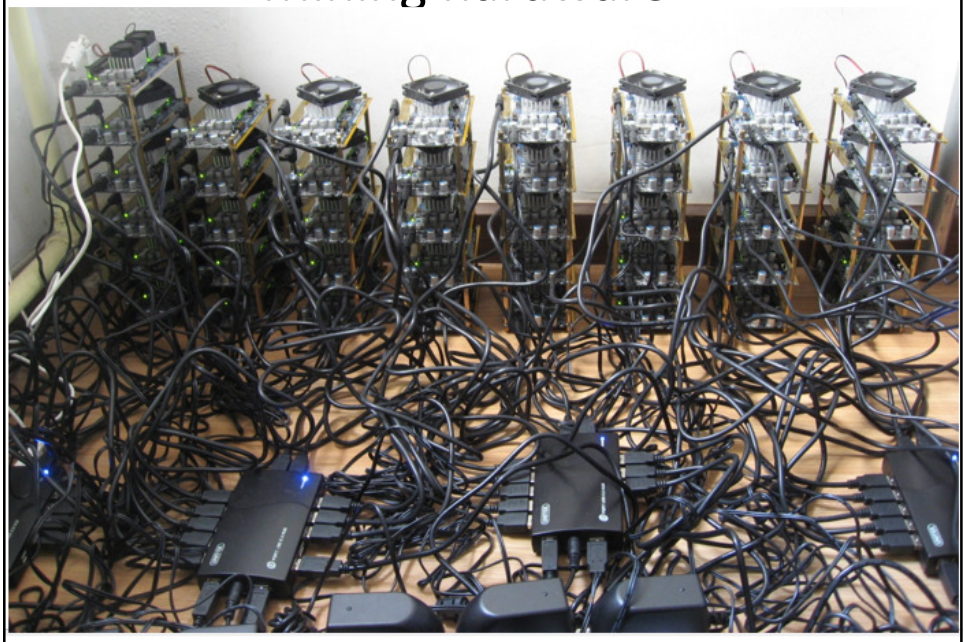
Grafic: număr de Hashes/secundă de-a lungul timpului

sursa: *https://blockchain.info*, mai 2021

Iulie 2010: 1 GHash/s
Octombrie 2010: 10 GHash/s
Decembrie 2010: 100 GHash/s
Mai 2011: 1 THash/s
Februarie 2012: 10THash/s
Iunie 2013: 100 THash/s
Sept. 2013: 1000 THash/s
Februarie 2016: 1M THash/s
Oct. 2019: 100M THash/s

28

Mining hardware



Se folosesc GPU-uri sau mai nou ASIC-uri

29

Mining hardware

Used Bitmain ANTMINER S19 PRO 110th/s BTC miner SHA-256 (3 Months Warranty)

Pre-Owned

$3,600.00

16 bids

5d 19h left (Monday, 11AM)

From China

Free international shipping

Watch

2021: echipament bazat pe ASIC-uri

Exemplu:

AntMiner S19

110 Tera Hash/s

consum electric: 3250W

eficiență: 30 J/Thash

profit: 0.00055 BTC/zi

echiv. mai 2021: 23$/zi

OBS: funcționează prin asocierea într-un mining pool

Profitability

Period	/day	/month	/year
Income	$32.62	$978.72	$11,744.65
Electricity	-$9.36	-$280.80	-$3,369.60
Profit	$23.26	$697.92	$8,375.05

30

Mining hardware

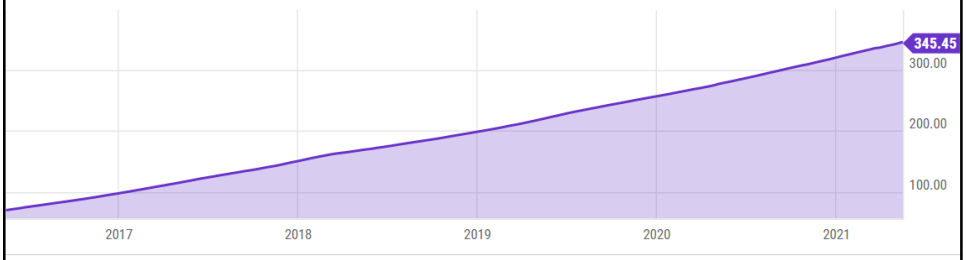
MODEL / CORES / FREQUENCY	HASH RATE	MONTHLY REVENUE
AMD Ryzen Threadripper 3970X 32-Core Processor / 64 / 3.69 GHz	19.9 kh/s	$45.11
Intel® Core™ i9-10900 / 20 / 2.80 GHz	4.17 kh/s	$9.44
Intel® Core™ i7 Q 740 / 8 / 1.73 GHz	148 h/s	$0.33

Exemple (mai 2021) de folosire a unor procesoare de uz general (folosind un soft de mining instalat pe un PC obișnuit)

Sursa: https://www.hashrates.com/cpus/

31

Statistici la nivel global



Dimensiunea Blockchain:

aprilie 2015: 30 GBytes aprilie 2016: 65 Gbytes

aprilie 2017: 111 Gbytes aprilie 2018: 165 Gbytes

aprilie 2019: 215 Gbytes aprilie 2020: 273 Gbytes

aprilie 2021: 340 GBytes

Consecință: descărcarea inițială a întregului Blockchain de către un utilizator nou este lentă.

32

Statistici la nivel global

Bitcoin Average Block Size	May 16 2021	1.372 MB
Bitcoin Average Confirmation Time	May 16 2021	135.70 min
Bitcoin Average Cost Per Transaction	May 16 2021	190.07 USD/tx
Bitcoin Average Cost Per Transaction	May 16 2021	0.0042 BTC/tx
Bitcoin Average Difficulty	May 16 2021	25.05 T
Bitcoin Average Transaction Fee	May 16 2021	11.23 USD/tx
Bitcoin Average Transaction Fee	May 16 2021	0.0002 BTC/tx
Bitcoin Average Transactions Per Block	May 16 2021	1662.39
Bitcoin Blockchain Size	May 16 2021	345.45 GB
Bitcoin Market Cap	May 16 2021	917.68B USD
Bitcoin Miners Revenue Per Day	May 16 2021	41.71M USD
Bitcoin Network Hash Rate	May 16 2021	164.35M TH/s
Bitcoin Supply	May 16 2021	18.71M BTC
Bitcoin Total Output Value Per Day	May 16 2021	1.828M BTC
Bitcoin Total Transaction Fees Per Day	May 16 2021	52.09 BTC
Bitcoin Total Transaction Fees Per Day	May 16 2021	2.465M USD
Bitcoin Total Transactions	May 16 2021	642.54M
Bitcoin Transactions Per Day	May 16 2021	219435.0

33

Consum electric la nivel global

Name	Population	Annual Electricity Consumption (TWh)
China	1,443M	6,543
United States	330.2M	3,989
All of the world's data centers	-	205
State of New York	19.3M	161
Bitcoin network	-	**129**
Norway	5.4M	124
Bangladesh	165.7M	70
Google	-	12
Facebook	-	5
Walt Disney World Resort (Florida)	-	1

- Consum anual, actualizat: mai 2021

34

Consum electric la nivel global

- imagine: „mining farm” → echivalent cu un datacenter
- numărul de mineri și de echipamente se extinde, dar eficiența echipamentelor crește, deci estimările variază enorm:
  - de la **18KWh per GHash/sec** cu un CPU de uz general
  - la **0.1Wh per GHash/sec** cu un ASIC

35

Probleme

1. Cum se implementează “avizierul” ?
2. Cum se identifică utilizatorii?
3. De unde provin banii?
4. Care e sintaxa tranzacțiilor?

36

Identificarea userilor

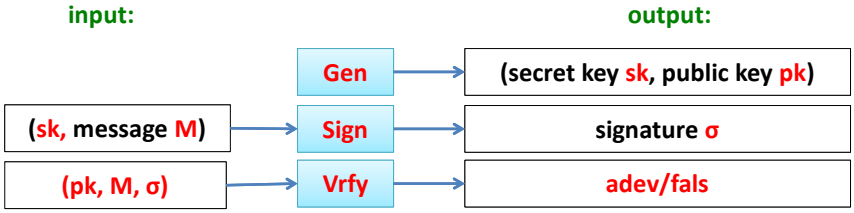
Se folosesc semnături digitale.

Se identifică tranzacțiile, nu userii, folosind cheile publice proprii (una per tranzacție)

37

Semnături digitale

O schemă de semnătură digitală conține algoritmii **Gen**, **Sign** și **Vrfy**



Verificare:

pentru fiecare **(sk,pk) := Gen()** și pentru fiecare **M** avem
Vrfy(pk,M,Sign(sk,M)) = adev

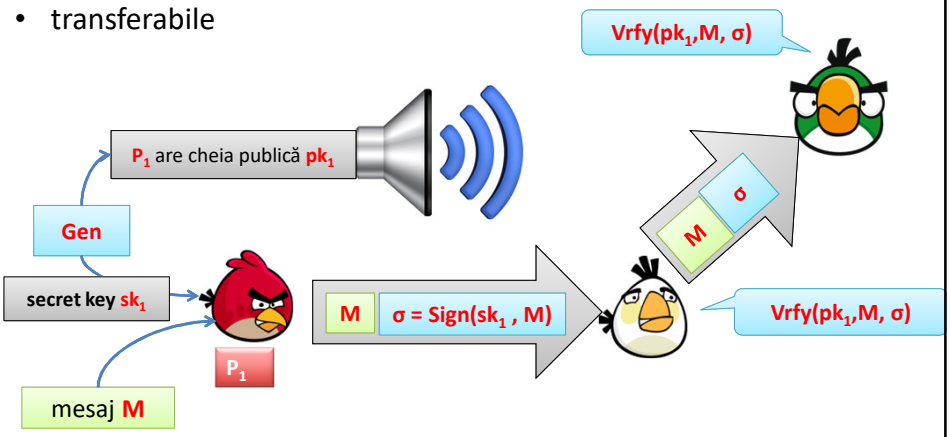
Securitate:

fără cunoașterea **sk** nu se poate calcula **σ** a.î. **Vrfy(pk,M,σ) = adev**

38

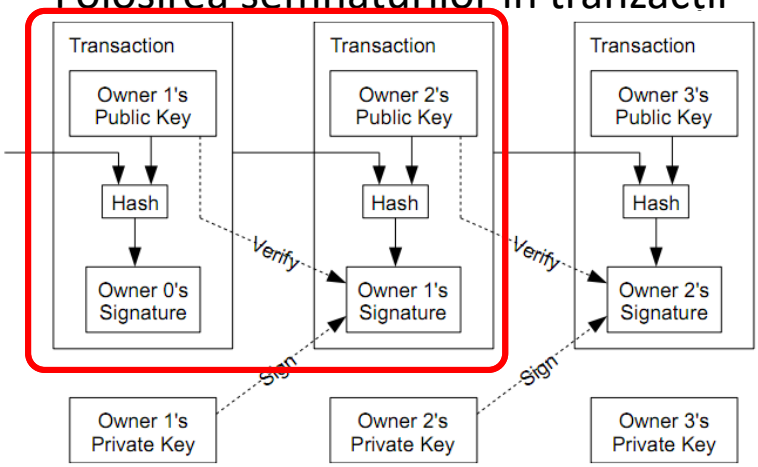
Avantajele semnăturilor digitale:

- verificabile public; oricine poate verifica căci pk este disponibil
- non-repudiabile; odată semnată, tranzacți rămîne
- transferabile



39

Folosirea semnăturilor în tranzacții



- O tranzacție reprezintă transferul unei sume de la Owner0 la Owner1, de la 1 la 2, de la 2 la 3 etc. Fiecare trz. e folosită ca intrare pt. hash în următoarea trz.
- **Trz cu roșu: Owner1 transferă către 2** adică Owner1 semnează tranzacția cu cheia sa *privată*. Cheia *publică* a lui Owner2 este efectiv „adresa" destinație a Bitcoins.
- Owner1 a semnat, oricine poate verifica aceasta, cheia publică a Owner1 fiind în tranzacția precedentă (0 → 1) din lanț; tranzacția nu mai poate fi anulată, fiind parte a unui lanț.

40

Probleme

1. Cum se implementează “avizierul” ?
2. Cum se identifică utilizatorii?
3. De unde provin banii?
4. Care e sintaxa tranzacțiilor?

41

De unde provin banii?

Un miner care găsește un bloc nou primește automat o recompensă în **BTC**:

la fiecare 4 ani, înjumătățire

- pt. primele **210 000** blocuri: **50 BTC/bloc**
- următoarele **210 000** blocuri: **25 BTC**
- următoarele **210 000** blocuri: **12.5 BTC**
- următoarele **210 000** blocuri **: 6.25 BTC** curent

etc…

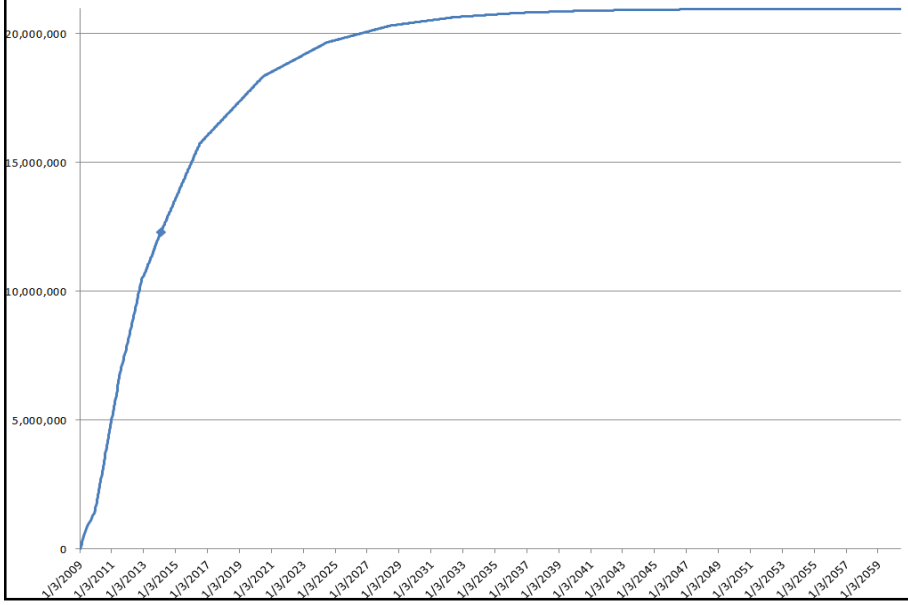
OBS1: 210 000 (50 + 25 + 12.5 + ⋯) = 21 000 000 BTC

OBS2: aprilie 2021: > 18 milioane BTC minați

OBS3: ultimii 7% din totalul BTC se vor mina în aprox. 100 ani!

42

Evoluție estimată a nr. de BTC



43

Recompense

Recompensa – o sumă fixă în BTC - se transferă către minerul care a creat noul bloc, prin *prima tranzacție din bloc*

<u>Avantaje</u>:

1.motivație pentru mineri.

2.minerii sînt interesați să rezolve problema criptografică a *hash*-ului și publice *(broadcasting)* **noul bloc** cît mai repede

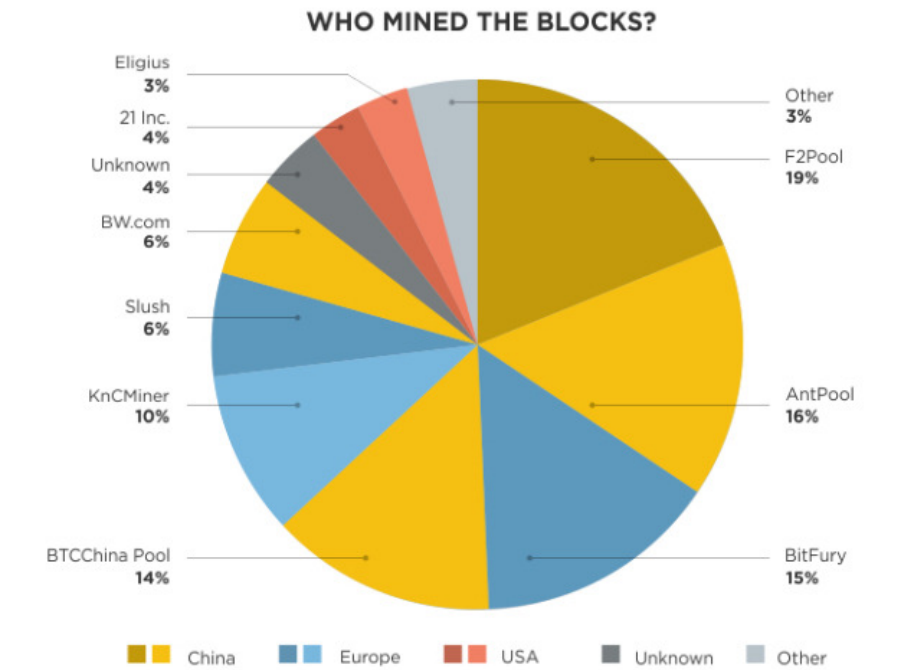
3.recompensa per bloc este singura cale de **a crea BTC noi în sistem**! orice altă tranzacție transferă BTC existenți!

44

Recompense

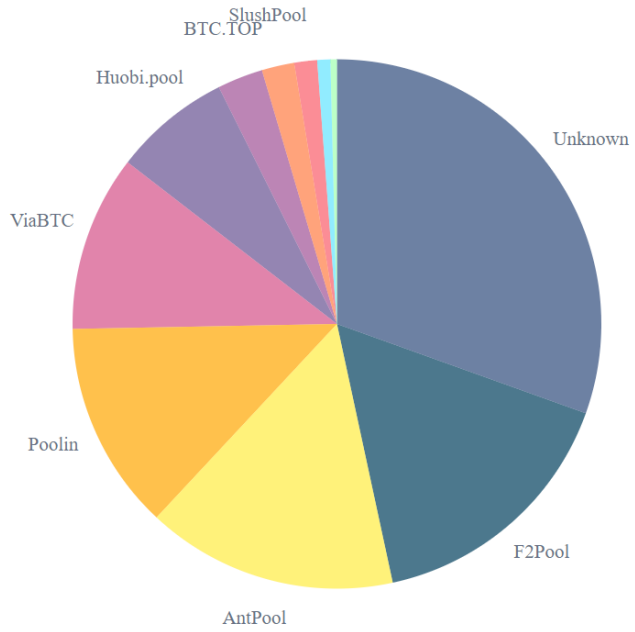
- Problemă probabilistică → șansele unui miner să găsească soluția înaintea oricărui altuia sînt mici; minerii se asociază în *miner guilds* sau *pools*, pun resursele hardware în comun și împart cîștigurile (vezi grafic următor: cele mai multe blocuri sînt create în cadrul *pools)*
- La fiecare 4 ani, recompensa se înjumătățește (2016 → 12.5 BTC; 2020 → 6.25 BTC
- Care va mai fi motivația minerilor în viitorul mai îndepărtat ?
  - Valoarea BTC crește (50 BTC în 2010 valorau *mult* mai puțini $ decît 6.25 BTC în 2021 !)
  - Tranzacțiile pot conține și *transaction fees*: la orice tranzacție să existe și o tranzacție adițională cu un *fee* către miner
  - tranzacțiile fără *fees* ar putea fi, ipotetic, ignorate.
  - tranzacțiile cu *fees* sînt procesate de mineri înaintea celor fără *fees* deci timpul de așteptare e invers prop. cu *fee.*

45



sursa: https://bitsonblocks.net/2015/09/21/a-gentle-introduction-to-bitcoin-mining/ (2015)

46



Actualizare mai 2021

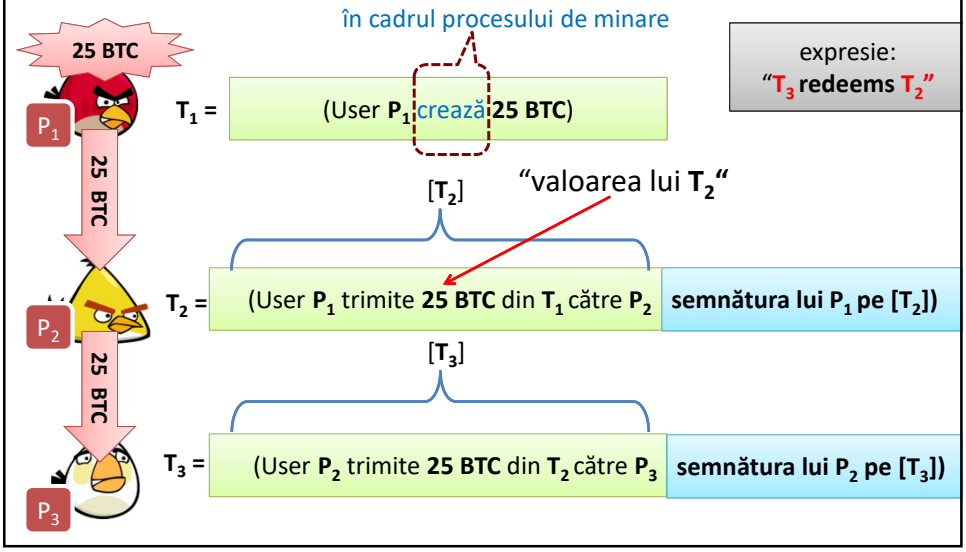
47

Probleme

1. Cum se implementează “avizierul” ?
2. Cum se identifică utilizatorii?
3. De unde provin banii?
4. Care e sintaxa tranzacțiilor?

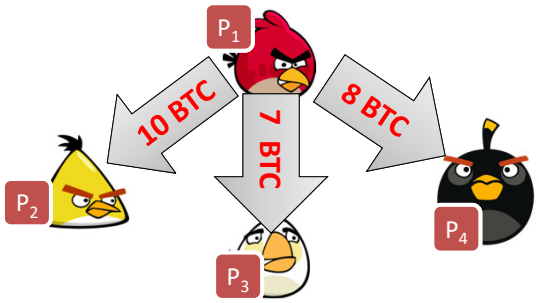
48

Sintaxa Tranzacțiilor



49

Divizarea banilor



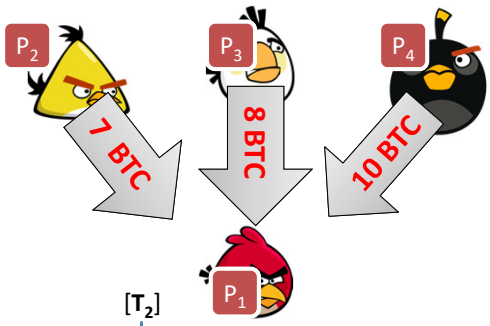
tranzacții cu ieșiri multiple (se plătește către mai mulți):

[T2]

T2 = (User P1 trimite 10 BTC din T1 către user P2 , User P1 trimite 7 BTC din T1 către user P3 , User P1 trimite 8 BTC din T1 către user P4 semnătura lui P1 pe [T2])

50

Intrări multiple



$[T_2]$

T_2 = (User P_2 trimite **10 BTC** din T_1 către user P_1 , User P_3 trimite **7 BTC** din T_1 către user P_1 , User P_4 trimite **8 BTC** din T_1 către user P_1 **semnătura lui P_2 pe $[T_2]$, semnătura lui P_3 pe $[T_2]$, semnătura lui P_4 pe $[T_2]$)**

toate semnăturile trebuie să fie valide!

51

Time-locks

se poate specifica timpul **t** cînd tranziția devine validă.

$[T_2]$

T_2 = (User P_1 trimite **25 BTC** din T_1 către P_2 dacă timpul **t** s-a scurs) **semnătura lui P_1 pe $[T_2]$)**

măsurat în:
- **unități de timp**, sau
- **blocuri**.

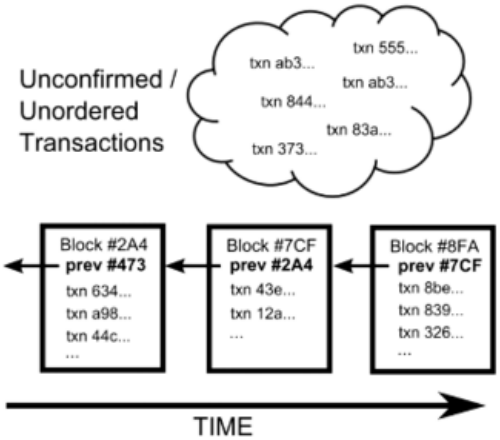
52

Time-locks

- Memento: prima tranzacție din bloc este tranzacția care crează BTC noi, către minerul care a generat blocul.
- Această tranzacție este *time-locked* pe o durată de 100 blocuri
- Deci, dacă blocul a fost creat greșit (într-un lanț prea scurt în cadrul unui *fork*, de exemplu), suma nu va putea fi colectată, căci nu vor urma 100 de blocuri după acel bloc greșit!

53

Înlănțuirea blocurilor (*blockchain)*



- Grupuri de tranzacții formează un bloc
- Tranzacțiile încă neconfirmate nu se află (încă) în nici un bloc
- Blocurile successive sînt înlănțuite a.î. un bloc să conțină o referință la blocul anterior; astfel se garantează că un bloc nou a apărut după blocul precedent; nu se pot genera și insera blocuri „ilicite”

54

Înlănțuirea blocurilor

- Tranzacțiile încă neconfirmate nu se află (încă) în nici un bloc
- Mempool size= dimensiunea tranzacțiilor încă neconfirmate. Ele conțin informație pentru mai multe zeci de blocuri (zeci de MB vs. cca 1MB per block).

55

Tranzacții și bani

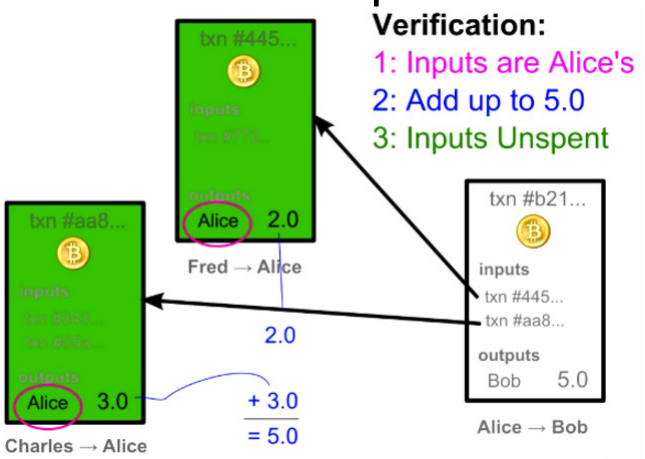
- Cînd Alice plătește 5BTC către Bob, cum verificăm cîți bani are Alice în „cont” ?
- A: Nu există „conturi” în sensul bancar obișnuit !

- Toți banii sînt referiți ca linkuri la tranzacții precedente
- Memento: banii sînt „creați” efectiv doar cînd un miner publică un bloc, deci *orice* șir de tranzacții are la origine o astfel de tranzacție de „creere a banilor”.

- Deci, Alice plătește către Bob prin tranzacții care să conțină linkuri către alte tranzacții care totalizează 5BTC!

56

Exemplu



- Alice plătește 5BTC către Bob
- Este o tranzacție cu output=Bob
- Provine din 2 tranzacții în care output=Alice (2 BTC și 3BTC), tranzacția include deci link la aceste 2 tranzacții anterioare
- Trebuie verificat și că cele 2 tranzacții sînt *unspent*

57

Exemplu

- Alice plătește 5BTC către Bob
- Verificarea că cele 2 input-uri de 2BTC și 3BTC sînt *unspent* (nu sînt input pentru nici o altă tranzacție) = să se evite *double spending*-ul
- Pentru a verifica că un input este *unspent*, trebuie verificate toate tranzacțiile precedente, pentru a vedea că nu folosesc acest input!
- Nodurile rețelei (minerii) fac aceste verificări, căci au nevoie de tranzacții verificate pentru a construi blocuri
- Sînt milioane de tranzacții precedente care trebuiesc verificate!
- Tranzacțiile *unspent* sînt menținute într-un index, pentru a permite verificarea rapidă.

58

Exemplu

- Alice plătește 5BTC către Bob
- 3+2 = 5

- Dar dacă Alice avea disponibile doar 2 tranzacții *unspent* de 3 și 4 BTC?
- 3+4 ≠5 !
- dar 3+4-2 = 5!
- deci pentru a plăti 5 BTC către Bob:
  - Alice plătește 3 către Bob
  - Alice plătește 4=(2 către Bob, 2 către ea-însăși)
- așadar, un total de 3 tranzacții în valoare de 7 BTC (2 tranzacții către Bob, o tranzacție către ea-însăși pentru a recupera „restul” de 2BTC)

59

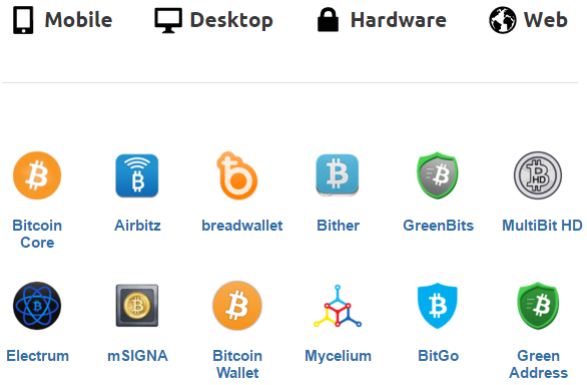
Generalizări

1. Valoarea totală a **in-coming transactions** poate fi mai mare decît a **out-going transactions**.
2. diferența este un comision (“**fee**”) **și este virat către miner**
3. se pot scrie și tranzacții condiționale folosind **Bitcoin scripting language** (**non-Turing complete** stack-based) - exemplu:

```
OP_DUP OP_HASH160
02192cfd7508be5c2e6ce9f1b6312b7f268476d2
OP_EQUALVERIFY OP_CHECKSIG
```

60

Portofelul de Bitcoini



- "**Bitcoin Wallet**"
- Sînt aplicații (de calculator, telef. mobil sau chiar dispozitiv dedicat) care permit generarea cheilor și tranzacțiilor de plată.
- Un „Full Node Wallet" descarcă întregul blockchain (> 100 GB) la instalare !
- Un „SPV Wallet" (*Simplified Payment Verification*) descarcă doar headerele blocurilor; se folosesc de nodurile „full" ale rețelei (minerii) pentru verificări.

61

Portofelul de Bitcoini

- "**Bitcoin Wallet**"
- Pentru o tranzacție, destinatarul banilor generează o pereche de chei (publică+privată)
- cheia publică este *adresa tranzacției* și se poate da sub formă de șir hexazecimal, un cod QR, cod de bare, etc. Un comerciant care vrea să primească BTC va publica ceva de forma:

1HLQ4vLRNnYE97SB6nRim9NL2aEBxPvXbk

- adresa tranzacției nu leagă tranzacția de o anumită persoană (*anonimitate*). O persoană va folosi alt set de chei pentru altă tranzacție, nu are un cont unic și personal, ca la bancă.
- cheia privată va fi folosită pt a cheltui în viitor BTC din tranzacție

62

Portofelul de Bitcoini - utilizare

- un vînzător acceptă bitcoins pentru un produs; el generează o pereche de chei și **transmite cumpărătorului cheia sa publică**, care este *adresa tranzacției* (destinația banilor)
- *OBS: cheia privată trebuie păstrată de vînzător pentru a folosi bitcoin-ii primiți din tranzacție: orice tranzacție ulterioară avînd ca input acei bitcoins va trebui semnată cu cheia privată respectivă - vezi slide „Folosirea semnăturilor în tranzacții" ; dacă se pierde, acei bitcoini sînt efectiv pierduți din sistem! (nimeni nu îi mai poate folosi ca input în nici o altă tranzacție). De aceea softul de portofel poate **proteja cu parolă** cheile private.*
- portofelul cumpărătorului **cere parola pentru a accesa cheile private** salvate odată cu tranzacții mai vechi, din care cumpărătorul a obținut bitcoins; *memento*: cumpărătorul nu are „bani", are „tranzacții vechi".
- portofelul se conectează la rețea și **transmite tranzacția** (tipic, TCP port 8333)
- vînzătorul **primește notificarea tranzacției** (neconfirmate încă) de la rețea și poate livra produsul imediat
- de obicei însă, așteaptă timp de 1..6 blocuri (10..60 minute) pentru a fi sigur că tranzacția e confirmată și nu s-a făcut *double spending*
- livrează produsul ! Tranzacția nu mai poate fi anulată.

63

Riscuri Bitcoin

1. Utilizarea BTC de către crima organizată


NEWS TECHNOLOGY

Home | UK | Africa | Asia | Europe | Latin America | Mid-East | US & Canada | Business | Health | Sci/E

28 January 2014 Last updated at 18:08 GMT

Share

US makes Bitcoin exchange arrests after Silk Road closure

"Silk Road" - site online gen eBay care vindea produse ilegale (inclusiv droguri), cu plata în Bitcoin; închis în 2013

Totuși, tranzacțiile în BTC pe Silk Road au dus la creșterea BTC.

64

2. Tranzacții ireversibile - risc de furt

Bitcoin firm Mt Gox wins brief US bankruptcy protection

65

3. Speculații despre "moartea Bitcoin"

- Periodic cineva anunță "moartea" inevitabilă a BTC
- pînă acum, toate au fost false "profeții"
- Bitcoin - comparat cu o "schemă Ponzi"

  Charles Ponzi, 1920: schemă piramidală; pe o idee similară a fost construit Caritas în anii '90 în România. Dar la Bitcoin nu există *intenția* de fraudare.
- Altă comparație: *Tulip Mania* - creșterea uriașă a prețului bulbilor de lalele în Olanda, 1630 (1 bulb de lalea *Semper Augustus* = 3000 guldeni; salariul anual al unui meșteșugar: 300 guldeni)
- Certitudine: între 2009 și 2021, apreciere față de dolar cu peste 10 000 000 % ! monedele „uzuale" nu variază atît de mult... implicit, factor de risc.

66

Alte “cryptocurrencies”

1	Bitcoin	$7,990,451,275		10	Feathercoin	$7,792,221	
2	Litecoin	$462,076,082		11	Primecoin	$6,755,642	
3	Auroracoin	$263,924,267		12	Infinitecoin	$5,925,613	
4	Peercoin	$70,470,621		13	Novacoin	$5,472,394	
5	Dogecoin	$56,320,267		14	Megacoin	$5,291,942	
6	Nxt	$44,237,970		15	Worldcoin	$3,368,914	
7	Namecoin	$28,621,193		16	Vertcoin	$3,334,443	
8	Quark	$9,715,693		17	Darkcoin	$3,268,761	
9	Protoshares	$9,429,425		18	Ybcoin	$2,887,990	

Toate se bazează pe principiile Bitcoin, cu modificări diferite (de ex. la Litecoin un bloc e terminat în 2.5 minute)

67

Bibliografie

Această prezentare este bazată pe materialul:

•Stefan Dziembowski (Univ. din Varșovia), *Cryptographic Aspects of Bitcoin*

Cu adausuri din alte resurse:

•Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*

•Jim Coman's Bitcoin Page, *http://www.coman.com/bitcoin/*

•Scott Driscoll, *“How Bitcoin Works Under the Hood”, http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html*

• A LOOK INSIDE AMERICA'S LARGEST BITCOIN MINING FARM: *https://www.youtube.com/watch?v=-ihMqEDs4B8*

68