

CureCoin: la blockchain per la ricerca

Fabio Mazza

Politecnico di Torino

Seminario del corso di Blockchain e Criptoconomia
2 luglio 2020



CureCoin



- CureCoin è una nuova criptovaluta (2014)
- Idea: riutilizzare la capacità di calcolo della blockchain

Introduzione

Gli ASIC hanno soppiantato le GPU nella Proof-of-Work:

- Gli ASIC sono molto efficienti (Hash/Watt) ma più costosi
- Ora, usare le GPU non è più economicamente sostenibile

Come risultato, molte GPU acquistate per il mining ora non sono più usate...

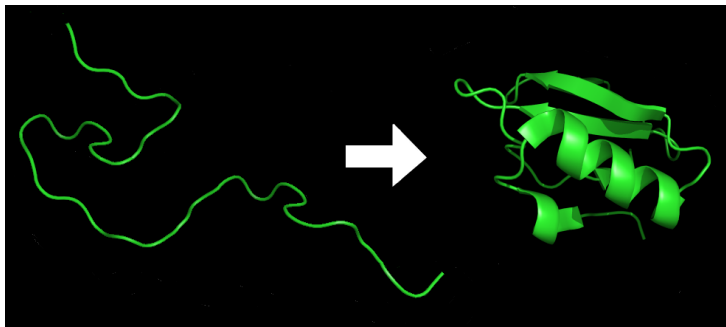
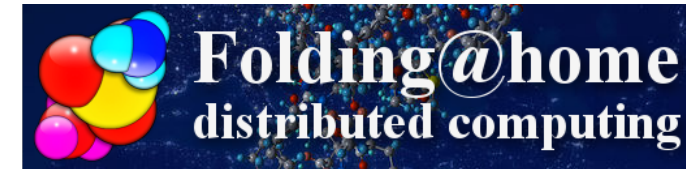
- Esistono altri ambiti in cui la loro potenza di calcolo può essere utile

Distributed Computing

- Molti ambiti della ricerca scientifica richiedono una gran quantità di calcoli:
 - Analisi dati (astrofisica)
 - Design di molecole (medicina)
 - Modelli climatici, ecc...
- Anziché usare supercomputer, si può dividere il lavoro tra molti pc anche poco potenti
- Negli anni, sono nati diversi programmi che permettono agli utenti di donare capacità di calcolo: BOINC (Berkeley), Folding@Home (Stanford)

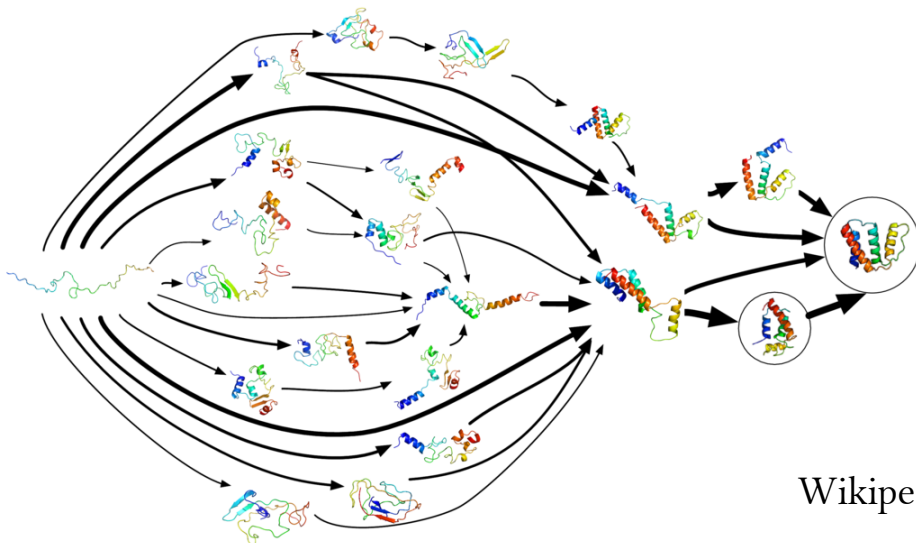
Folding@Home

- Programma di calcolo distribuito tramite Internet
- Protein Folding:
 - La forma delle proteine determina la funzione
 - Dalla sequenza della proteina, trovare la forma finale
 - Molte possibili forme finali, solo una è quella giusta
 - Forma sbagliata delle proteine alla base di malattie come Alzheimer, Huntington, cancro
- Problema con una complessità molto elevata



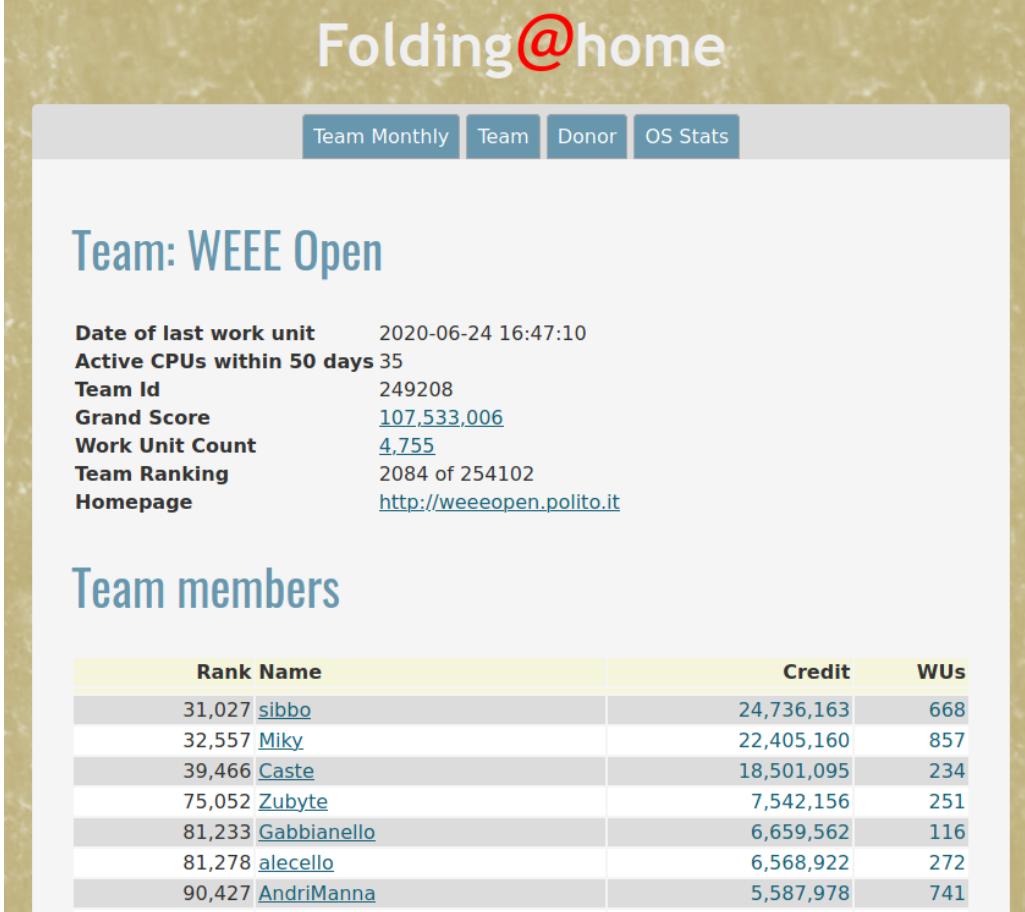
Folding@Home

- Nato ad Ottobre 2000, ha accumulato molti record di potenza di calcolo (1 petaFLOPS – 2007, 1.5 exaFLOPS x86 – Marzo 2020)
- Importante ondata di contributi a Marzo per la ricerca su Sars-CoV-2
- Simulazione del processo di folding: lavoro diviso tra CPU e GPU (anche PlayStation 3 in passato)



Contributi a Folding@Home

- Utenti (*folders*) ricevono Work Units (WU) per CPU o GPU
- Utenti completano le WU e le inviano ai server di F@H che ne valutano la validità
- Si ricevono punti (*Credit*) per ogni WU completata (di più se si finisce in fretta)
- Ranking **pubblico** dei *folders*, dettagli sui contributi
- Possibilità di formare team



The screenshot shows the Folding@home website interface for a team named 'WEEE Open'. At the top, there are navigation tabs: 'Team Monthly', 'Team', 'Donor', and 'OS Stats'. Below the team name, several statistics are listed: 'Date of last work unit' (2020-06-24 16:47:10), 'Active CPUs within 50 days' (35), 'Team Id' (249208), 'Grand Score' (107,533,006), 'Work Unit Count' (4,755), 'Team Ranking' (2084 of 254102), and 'Homepage' (http://weeeopen.polito.it). Below this, there is a section titled 'Team members' which contains a table with three columns: 'Rank Name', 'Credit', and 'WUs'.

Rank	Name	Credit	WUs
31,027	sibbo	24,736,163	668
32,557	Miky	22,405,160	857
39,466	Caste	18,501,095	234
75,052	Zubyte	7,542,156	251
81,233	Gabbianello	6,659,562	116
81,278	alecello	6,568,922	272
90,427	AndriManna	5,587,978	741

➡ Sistema a punti aumenta la competizione tra gli utenti

CureCoin e Folding@Home

- Ricompensa monetaria: in CURE, la moneta di CureCoin
- Divisione di un numero fissato di CURE tra i *folders*:
 - Utenti si uniscono al team CureCoin
 - Username F@H viene collegato all'indirizzo CureCoin
 - Ricompensa giornaliera proporzionale ai punti guadagnati
- Il numero totale di CURE così distribuiti viene dimezzato periodicamente (*halving*)
- Le ricompense dei *folders* sono già *minted* (no generazione di nuova moneta)

CureCoin e Folding@Home

Il sistema di Folding@Home è centrale:

- Fornisce un ranking pubblico
- Verifica tutte le Work Units caricate
- Incentiva i *folders* a finire in fretta le WU
- I punti bonus vengono assegnati solo se l'utente si comporta bene (*dumping* delle WU)

Meccanismo di consenso

- Nella prima versione, principalmente Proof-of-Work (ASIC, fino al 2018)
- Nella v2, solo Proof-of-Stake (hard fork)
- Proof-of-Stake come Peercoin:
 - *Coin age* (tempo × valore in coins)
 - Difficoltà di calcolo dell'hash diminuisce con la *coin age*
 - Tentativo di calcolo hash riuscito: il miner paga a se stesso il 101% dei coin che ha usato ⇒ reset età
 - Minimo e massimo età dei coins

Meccanismo di consenso

- In CureCoin, età massima dei coins di 90 gg, minima di 30 gg
- Recentemente, età minima dei coins portata a 4 gg e ricompensa del 4% per Proof-of-Stake \Rightarrow incentivare *staking* tra gli utenti
- Ricompense del *folding* in diminuzione \Rightarrow alla fine lo *staking* sarà il principale meccanismo di distribuzione dei CURE
- Previsioni rewards (del 2018 – dei dev CureCoin):
 - Fino al 2021: 70% ricompense al *folding*, 30% *staking*
 - 2021 – 2025: 45% *folding*, 55% *staking*
- Ricompensa per lo *staking* sarà diminuita.

Ricompense

100 Years of Mintage (Curecoin 2.0 - Draft) : 100 Yrs of Mintage (no stake halving) 4/8/19

ATTENTION: Today's Curecoin 2.0 Proof-of-Stake architecture will not be sustained beyond 12/5/2021 halving period. Expect future Hardforks with low (or no!!!) Proof-of-Stake. Current returns are no guarantee of future performance - PoR 05/29/2019

Key dates	Event	Daily folding rewards	Avg stake coins / day est.	Starting block height	Num days per halving	Months/halving	Blocks per day	Average Staking coins per block	Total folding reward coins per halving	Folding distribution % per halving	Total stake coins earned per halving	Staking distribution % per halving (post-HF)	*annual* staking percentage of total distribution	Total reward per halving	total coins in circulation (end of halving)
12/21/2018	HF	3744.000	1600.4782	257322	1080	35.5	360	4.44577285	4043520.0	70.05%	1728516.48	29.95%	4.42%	5772036.48	16,168,194.81
12/5/2021	halving	1872.000	2317.0553	646122	1460.0	47.9	360	6.43626462	2733120.0	44.69%	3382900.69	55.31%	4.42%	6116020.69	22,284,215.50
12/4/2025	halving	936.000	3039.3587	1171722	1460.0	47.9	360	8.44266312	1366560.0	23.55%	4437463.74	76.45%	4.42%	5804023.74	28,088,239.24
12/3/2029	halving	468.000	3764.2249	1697322	1460.0	47.9	360	10.45618014	683280.0	11.06%	5495768.28	88.94%	4.42%	6179048.28	34,267,287.52
12/2/2033	halving	234.000	4560.7073	2222922	1460.0	47.9	360	12.66863128	341640.0	4.88%	6658632.60	95.12%	4.42%	7000272.60	41,267,560.12
12/1/2037	halving	117.000	5476.9341	2748522	1460.0	47.9	360	15.21370585	170820.0	2.09%	7996323.80	97.91%	4.42%	8167143.80	49,434,703.91
11/30/2041	halving	58.500	6553.2010	3274122	1460.0	47.9	360	18.20333622	85410.0	0.88%	9567673.52	99.12%	4.42%	9653083.52	59,087,787.43
11/29/2045	halving	29.250	7829.0263	3799722	1460.0	47.9	360	21.74729528	42705.0	0.37%	11430378.40	99.63%	4.42%	11473083.40	70,560,870.83
11/28/2049	halving	14.625	9347.2853	4325322	1460.0	47.9	360	25.96468134	21352.5	0.16%	13647036.51	99.84%	4.42%	13668389.01	84,229,259.84
11/27/2053	halving	7.313	11157.0022	4850922	1460.0	47.9	360	30.99167269	10676.3	0.07%	16289223.16	99.93%	4.42%	16299899.41	100,529,159.25
11/26/2057	halving	3.656	13315.6102	5376522	1460.0	47.9	360	36.98780609	5338.1	0.03%	19440790.88	99.97%	4.42%	19446129.00	119,975,288.26
11/25/2061	halving	1.828	15891.1134	5902122	1460.0	47.9	360	44.14198166	2669.1	0.01%	23201025.56	99.99%	4.42%	23203694.62	143,178,982.88
11/24/2065	halving	0.914	18964.3986	6427722	1460.0	47.9	360	52.67888505	1334.5	0.00%	27688021.98	100.00%	4.42%	27689356.52	170,868,339.39
11/23/2069	halving	0.457	22631.8607	6953322	1460.0	47.9	360	62.86627961	667.3	0.00%	33042516.56	100.00%	4.42%	33043183.83	203,911,523.22
11/22/2073	halving	0.229	27008.4682	7478922	1460.0	47.9	360	75.02352264	333.6	0.00%	39432363.50	100.00%	4.42%	39432697.13	243,344,220.35
11/21/2077	halving	0.114	32231.3888	8004522	1460.0	47.9	360	89.53163569	166.8	0.00%	47057827.72	100.00%	4.42%	47057994.53	290,402,214.89
11/20/2081	halving	0.057	38464.2992	8530122	1460.0	47.9	360	106.84527558	83.4	0.00%	56157876.84	100.00%	4.42%	56157960.25	346,560,175.14
11/19/2085	halving	0.029	45902.5190	9055722	1460.0	47.9	360	127.50699727	41.7	0.00%	67017677.76	100.00%	4.42%	67017719.47	413,577,894.61
11/18/2089	halving	0.014	54779.1347	9581322	1460.0	47.9	360	152.16426316	20.9	0.00%	79977536.72	100.00%	4.42%	79977557.57	493,555,452.17
11/17/2093	halving	0.007	65372.3049	10106922	1460.0	47.9	360	181.58973586	10.4	0.00%	95443565.17	100.00%	4.42%	95443575.60	588,999,027.77
11/16/2097	halving	0.004	78013.9772	10632522	1460.0	47.9	360	216.70549230	5.2	0.00%	113900406.75	100.00%	4.42%	113900411.96	702,899,439.73
11/16/2101	halving	0.002	93100.2908	11158122	1460.0	47.9	360	258.61191880	2.6	0.00%	135926424.52	100.00%	4.42%	135926427.13	838,825,866.86
11/15/2105	halving	0.001	102662.2778	11683722	176.0	5.8	360	285.17299387	0.2	0.00%	18068560.89	100.00%	4.42%	18068561.05	856,894,427.91
5/10/2106	*final block based on original schedule			11747082					9509757.6					846498269.58	←total 2.0 distribution (88 years)
†original 1.0 final block 5045760 reached in ~2058									†remaining folding rewards since HF					10396158.33	est. total 1.0 in circulation n
In this model, halving periods continue from 1.0 schedule									Halving Period 4,000 years					856894427.91	Total distribution 1.0 + 2.0
*This is a draft document for the Plan of Record (PoR) as of 05/29/2019 ... Expect ongoing updates									Dev coins 819935.9511						
									Donor coins 541390						
									→					1361325.951	total non-folder 1.0 premine
														858255753.86	Total Distributions + non-fol

Vantaggi di CureCoin

Rispetto a Bitcoin:

- Le ASICs risultano svantaggiate nel mining
- La potenza computazionale impegnata è quasi interamente usata per la ricerca
- Velocità maggiore nella validazione, coinvolgimento maggiore degli utenti (PoS)
- Un blocco viene generato ogni 4 minuti (Bitcoin: 10 minuti)

Caratteristiche di CureCoin

Come Bitcoin:

- E' una criptovaluta dotata di propria blockchain
 - Esiste un numero massimo di CureCoin ottenuti con il *folding*
- ➔ Ha avuto un discreto successo (1° team su Folding@Home, più di 27 M di Work Units completate, 470 teraFLOPS di potenza di calcolo)

Team Statistics			
Name	is exactly ▼	<input type="text"/>	
Team #		<input type="text"/>	<input type="button" value="Search"/>
Rank	Name	Credit	WUs
Team			
Top 100			
1	Default (No team specified)	1,227,740,208,412	234,993,948
2	Curecoin	1,208,489,920,332	27,915,640
3	LinusTechTips_Team	520,593,602,426	22,294,025
4	folding@evga	400,570,155,940	29,431,662
5	Hardware.no	156,003,163,785	10,169,641

Caratteristiche di CureCoin

Curecoin Charts



coinmarketcap.com

Conclusioni

- Curecoin ritorna ad utilizzare le GPU
- Aggiunge valore etico alla criptovaluta
- Progetto indipendente da Folding@Home, ma incardinato su F@H

In futuro:

- Utilizzo di altre reti di calcolo distribuite, oltre a Folding@Home
- Aggiunta di funzionalità alla blockchain (salvataggio dei documenti, per esempio)
- Sicurezza (Merkle signatures)



Grazie per l'attenzione

Fonti e link utili

- ▶ [Pagina di Wikipedia su Folding@Home](#)
- ▶ [Statistiche Folding@Home](#)
- ▶ [CureCoin "Whitepaper"](#)
- ▶ [CureCoin Knowledge Base](#)
- ▶ [Distribuzione CureCoins](#)
- ▶ [Roadmap CureCoin](#)
- ▶ [Piano della distribuzione di CureCoin nel futuro](#)
- ▶ [Thread su reddit su PoW e PoS in CureCoin](#)
- ▶ [Peercoin Whitepaper, Sunny King, Scott Nadal, 2012](#)