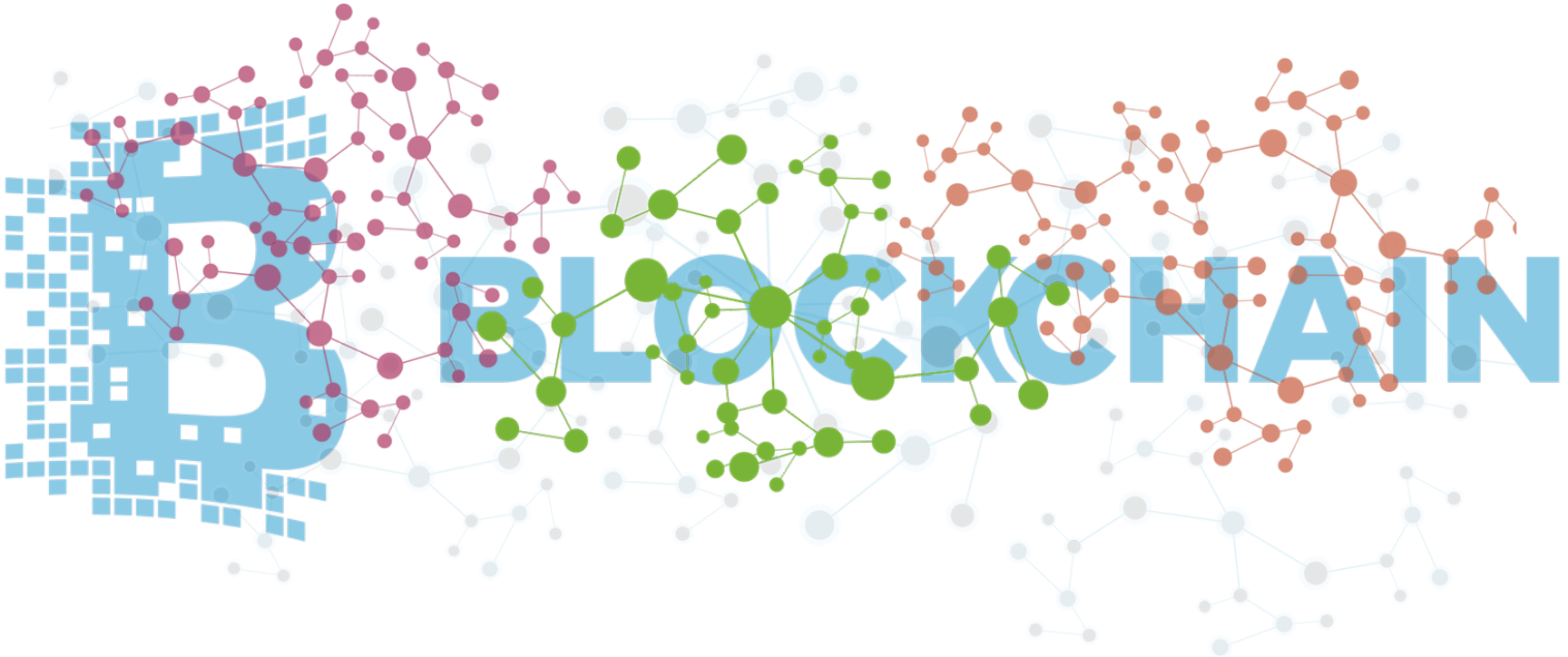


PROGETTO UCAL

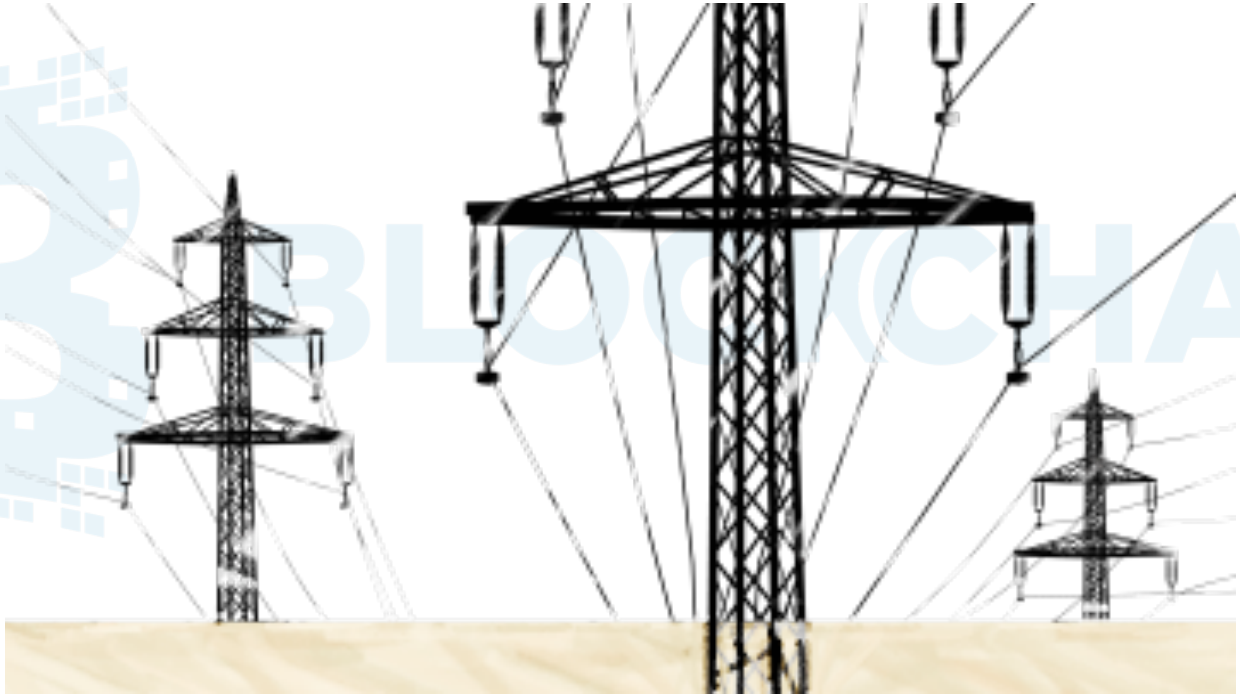
NTT DATA
Global IT Innovator

Blockchain Governance

www.blockchain.srl

Pastorelli, Rende, Giugno, 2016

CONSUMI ENERGETICI NELLA GESTIONE DEL MINING

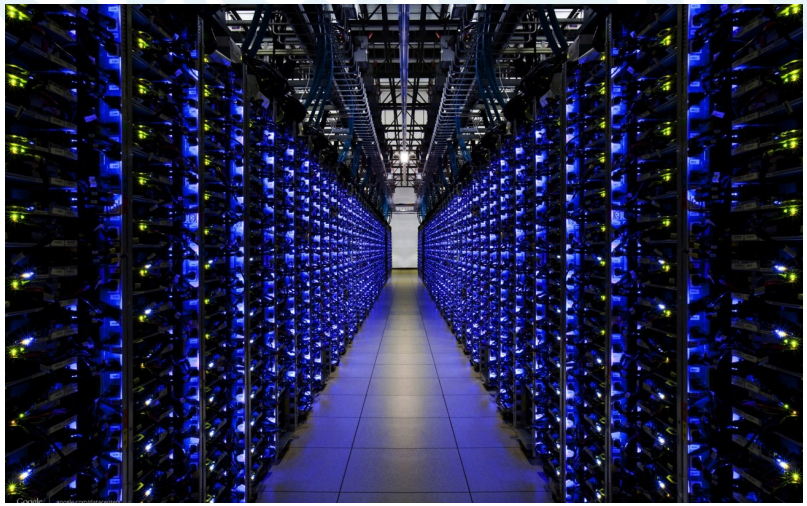


Definizione di blockchain

«La definizione tecnica è ” libro mastro decentralizzato e crittograficamente sicuro di transazioni”. Più in generale, possiamo dire che è una tecnologia che permette di scambiare su internet non solo informazioni ma, per la prima volta, anche proprietà. Non solo il pagamento o lo scambio di beni e servizi, ma qualsiasi altra forma di collaborazione tra uomini potrà approfittare delle possibilità offerte dalla rete, grazie a questa innovazione. La differenza con altri sistemi peer-to-peer, come ad esempio Bittorrent, che viene usato per scambiare file musicali o video in rete, è la scarsità: un bitcoin, a differenza di un file mp3, non è infinitamente riproducibile, non è duplicabile. Non ne potranno nemmeno essere creati di nuovi in quantità infinita: i bitcoin contenuti nel protocollo sono come l’oro in una miniera, che contiene solo una quantità predefinita di metallo, dopo di che si esaurisce».

Processo di mining

«Per chi ha i mezzi necessari è possibile produrli, o meglio “estrarli”, aiutando a mettere al sicuro la rete tramite la risoluzione di complessi “enigmi” crittografici. Come si fa? Con un software libero e con (costosi) circuiti stampati ad hoc, mettendo quindi a disposizione una potenza di calcolo molto elevata. Chi risolve gli “enigmi” ed “estrae” i bitcoin, mettendo così al sicuro la rete, si chiama in gergo “miner” (minatore), proprio perché come un minatore deve tirare fuori una risorsa che esiste in quantità finita (e sempre più scarsa) dalla miniera dalla rete.



Mining BitCoin

Il protocollo di Bitcoin è prevalentemente basato su tecnologie già disponibili ed utilizzate prima della sua creazione, tra cui:

Crittografia Asimmetrica: una tecnologia crittografica davvero molto diffusa, che consente di identificare l'autore di un messaggio: Ogni utente possiede una chiave pubblica e una privata (nota unicamente a lui) per criptare un messaggio che sarà poi possibile decriptare unicamente usando la sua chiave pubblica, così che sia possibile ricondurre la creazione del messaggio direttamente a lui.

Crittografia di Hash: Una funzione che si occupa di creare un'impronta digitale unica e non reversibile di un file o di un messaggio. Esempio: Il testo "Satoshi Nakamoto" crittografato in hash MD5 è 45a872a13366071d5e1e5788c8eb4888, ma è impossibile risalire al testo dal numero, salvo provare ogni singola combinazione possibile.

Mining BitCoin

Dal punto di vista tecnico il processo di mining non è altro che un'operazione di hashing inverso: determinare un numero tale per cui l'hash SHA-256 di un insieme di dati rappresentante il blocco sia inferiore a una soglia data. Questa soglia, chiamata per l'appunto difficoltà, è ciò che determina la natura concorrenziale del mining di bitcoin: più potenza di calcolo viene aggiunta alla rete bitcoin e più questo parametro aumenta, aumentando di conseguenza il numero di calcoli mediamente necessari a creare un nuovo blocco e aumentando quindi il costo di creazione dello stesso, spingendo i nodi a migliorare l'efficienza dei loro sistemi di mining per mantenere un bilancio economico positivo. L'aggiornamento di questo parametro avviene ogni 14 giorni circa, dimensionandosi in modo che un nuovo blocco venga generato in media ogni 10 minuti

Tutti i nodi della rete competono per essere i primi a trovare una soluzione di un problema crittografico che riguarda il blocco candidato, un problema che non può essere risolto in altri modi che tramite bruteforce e che quindi richiede sostanzialmente un enorme numero di tentativi. Quando un nodo trova una soluzione valida l'annuncia al resto della rete attribuendosi contemporaneamente i bitcoin in premio previsti dal protocollo, i nodi che ricevono il nuovo blocco lo verificano e lo aggiungono alla loro catena, ricominciando il lavoro di mining al di sopra del blocco appena ricevuto.

Consumi e costi mining BitCoin

Antminer S7 ~4.73TH/s @ .25W/GH 28nm ASIC Bitcoin Miner

S7 Specifications:
1. Hash Rate: 4.73 TH/s ±5%
2. Power Consumption: 1293W ±10%
3. Power Efficiency: 0.25 W/GH ±10%
4. Rated Voltage: 11.60 ~13.00V
5. Chip quantity per unit: 135x BM1385
6. Dimensions: 301mm(L)*123mm(W)*155mm(H)
7. Cooling: 1x 12038 fan
8. Operating Temperature: 0 °C to 40 °C
9. Network Connection: Ethernet
10. Default Frequency: 700M

COSTO MACCHINA 550 USD

Consumi e costi mining BitCoin

Antminer S7 ~4.73TH/s @ .25W/GH 28nm ASIC Bitcoin Miner

CLIENTI RESIDENTI (COSTO KW)

Consumo annuo	3 kw	4,5 kw	6 kw
900 kwh >>	€ 0,18	€ 0,36	€ 0,39
1.200 kwh >>	€ 0,17	€ 0,33	€ 0,35
2.100 kwh >>	€ 0,17	€ 0,29	€ 0,30
2.700 kwh >>	€ 0,18	€ 0,28	€ 0,29
3.300 kwh >>	€ 0,20	€ 0,27	€ 0,28
3.900 kwh >>	€ 0,22	€ 0,28	€ 0,29
4.500 kwh >>	€ 0,24	€ 0,28	€ 0,29

Conusmo singola macchina 11300 kWh/anno

Consumi e costi mining BitCoin

4.73 Thash/s @ 196061423940 Difficulty

Hardware Break Even:	*-34694659.148 seconds*	Mhash/s per Watt:	*3658.16 Mhash/s*
Avg Time to Solve Block:	*5.6 years*	Avg Time per Share:	*0.001 s*

Average Results per Hour Day Week Month Text Format

Shares:	*2894187346*	Mining Result	*BTC 0.36904090*	*(EUR 190.66)*
		Power Cost	*BTC 0.43848292*	*(EUR 226.53)*
		Total Expected Result	*BTC -0.06944203*	*(EUR -35.88)*

PROGETTO UCAL

NTT DATA Global IT Innovator

Blockchain Governance

www.blockchain.srl

Pastorelli, Rende, Giugno, 2016

Consumi e costi mining BitCoin

4.73 Thash/s @ 196061423940 Difficulty

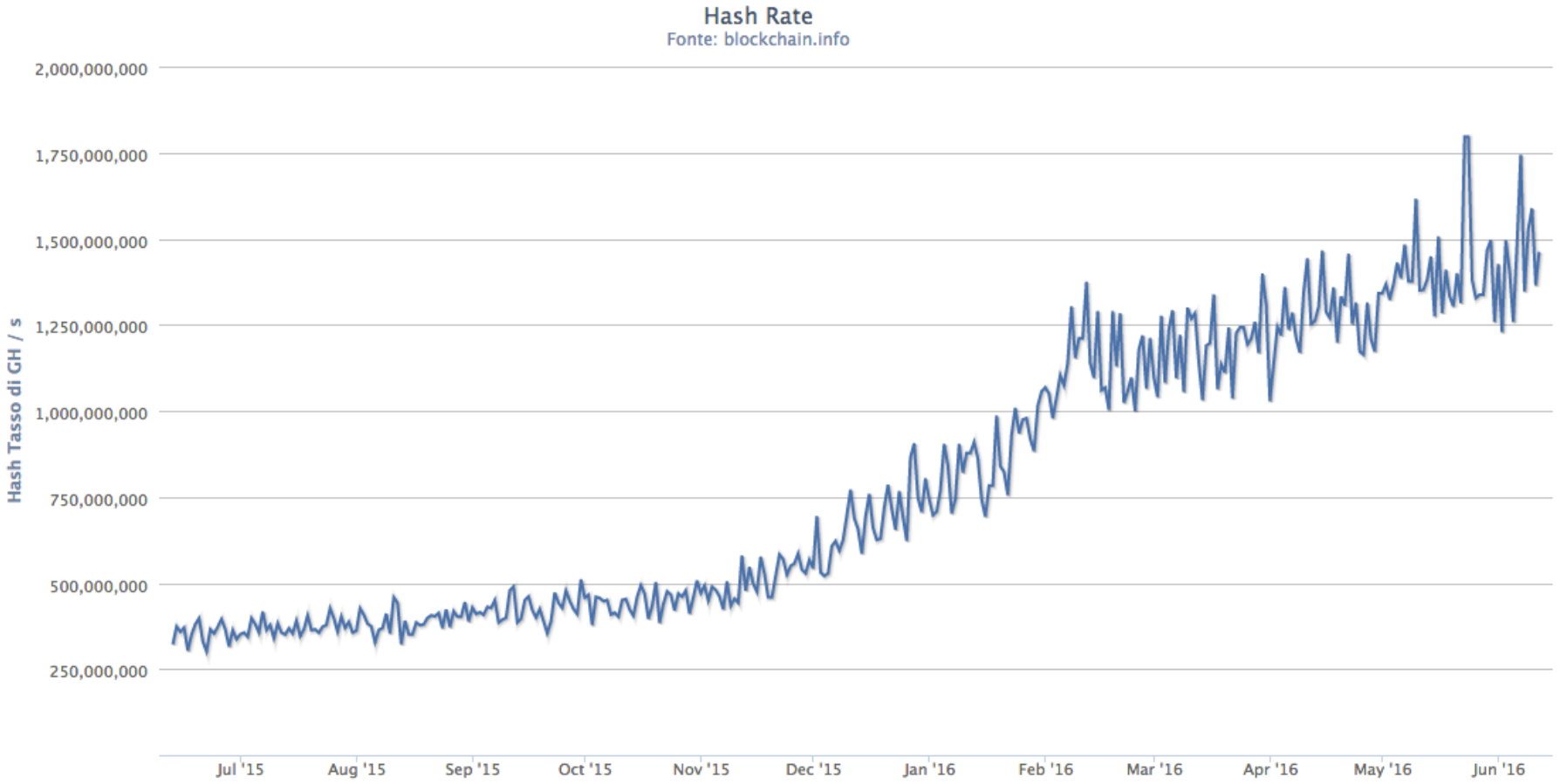
Hardware Break Even:	*128.3 days*	Mhash/s per Watt:	*3658.16 Mhash/s*
Avg Time to Solve Block:	*5.6 years*	Avg Time per Share:	*0.001 s*

Average Results per Hour Day Week **Month** Text Format

Shares:	*2894187346*	Mining Result	*BTC 0.36904090*	*(EUR 190.66)*
		Power Cost	*BTC 0.15164201*	*(EUR 78.34)*
		Total Expected Result	*BTC 0.21739889*	*(EUR 112.31)*

Singola macchina installata a Shanghai costo energia 0,61Y/kWh 0,083 EUR/kWh

Consumi e costi mining BitCoin



PROGETTO UCAL

NTT DATA Global IT Innovator

Blockchain Governance

www.blockchain.srl

Pastorelli, Rende, Giugno, 2016

Consumi e costi mining BitCoin
Analisi mining vs banking

Hass McCook
Chartered Engineer, Oxford MBA, Bitcoin
Educator & Researcher

Consumi e costi mining BitCoin
Analisi mining vs banking

Financial Access Point	Number per 100,000 adults (World Average)	Rationalised Number
Bank Branches	11.7	591,075 branches
ATMs	34.21	2,394,700 ATMs

Table 15 - World Bank Financial Access Data - 2014 (World Bank, 2014)

Access Type	Impact (million tonnes CO_2 / year)	Energy Use (GJ)
Bank Branches	383.1	2.3 billion
Automatic Telling Machines	3.2	18.9 million
Total	**386.3**	**2.3 billion**

Table 18 - Summary of Impact of World's Banking and Finance Access Points

Consumi e costi mining BitCoin
Analisi mining vs banking

Comparison of Environmental Costs

	Energy Used (GJ)	Tonnes CO_2 Produced	Emission Trend
Gold Mining	475 million	54 million	Increasing
Gold Recycling	25 million	4 million	Decreasing
Paper Currency & Minting	39.6 million	6.7 million	Increasing
Banking System	2340 million	390 million	Increasing
Bitcoin Mining	3.6 million	0.6 million	Decreasing

Ethereum e blockchain

Lo sviluppo di Ethereum è iniziato nel dicembre 2013, e le prime versioni del software sono state rilasciate agli inizi del febbraio 2014 Da allora sono state pubblicate diverse versioni successive, che hanno incluso lo sviluppo di tre linguaggi di programmazione appositamente creati per scrivere smart contracts.

Per finanziare il lavoro di sviluppo, Ethereum ha lanciato un'offerta pubblica di pre-vendita di Ether. L'offerta pubblica è durata 42 giorni ed ha totalizzato la raccolta di 31.591 Bitcoin, pari (al tasso di cambio del 2 settembre 2014) a circa 18,4 milioni di dollari statunitensi, o 60.102.216 ETH.

Ethereum mining

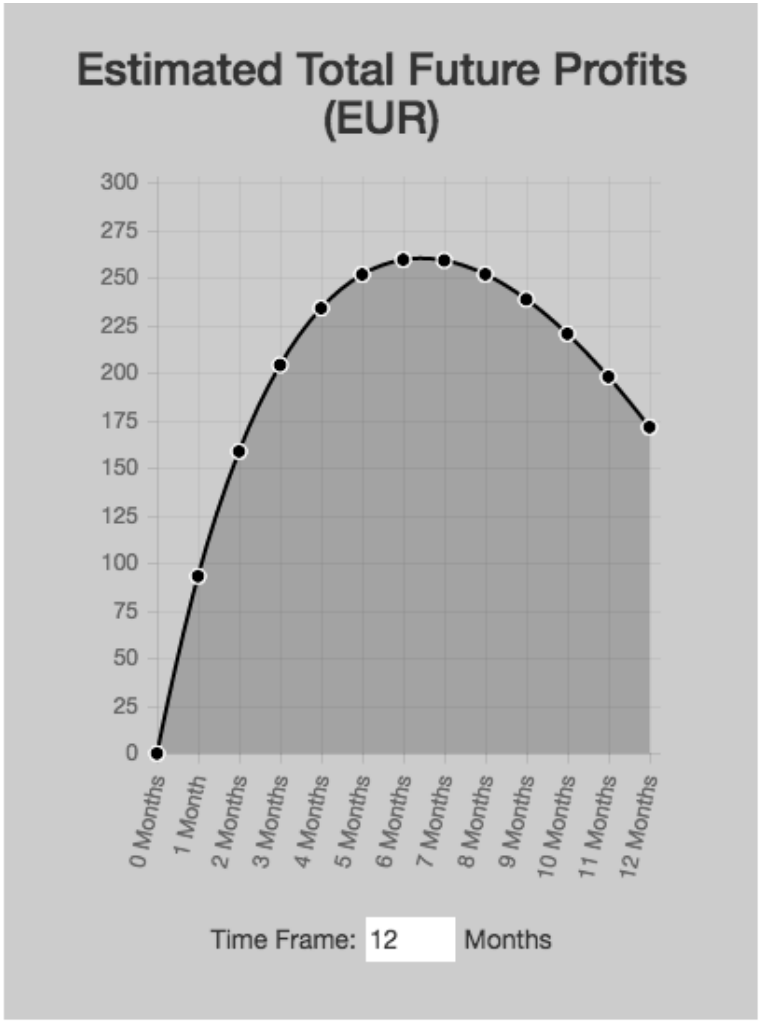
- ✓ Pc dotato di almeno 8 Gb di ram
- ✓Scheda video Radeon R9 295x2 hashrate 51Mh/s
- ✓Ethminer

Ethereum mining

Hashrate:	51	MH/s
Difficulty:	45,9973	Trillion
Block Time:	14,394	Seconds
ETH Price:	12,84	EUR
Power:	500	W
Power Cost:	0.24	EUR / kWh
Pool Fee	0	%
Diff Change	8,33	Trillion / Month

Profits At This Difficulty

Period	ETH	EUR	Power Cost (EUR)	Pool Fees (EUR)	Profit (EUR)
Hourly	0.02	$0.25	$0.12	$0.00	$0.13
Daily	0.47	$5.98	$2.88	$0.00	$3.10
Weekly	3.26	$41.87	$20.16	$0.00	$21.71
Monthly	13.98	$179.45	$86.40	$0.00	$93.05



PROGETTO UCAL

NTT DATA Global IT Innovator

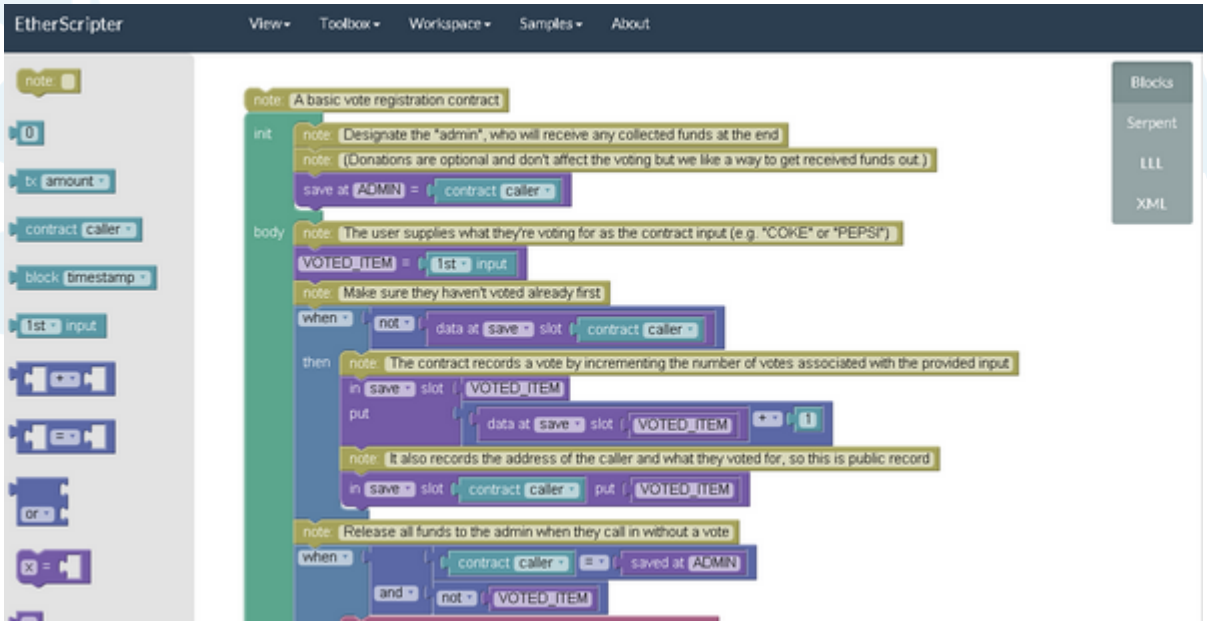
Blockchain Governance

www.blockchain.srl

Pastorelli, Rende, Giugno, 2016

Ethereum e blockchain non solo mining

- Smart Contracts non sono altro che dei programmi. Il loro codice o Ethereum virtual machine code (EVM code), contenuto all'interno delle transazioni, è scritto in linguaggio low-level e consiste in una serie di bytes, dove ogni byte rappresenta un operazione.



Ethereum e blockchain non solo mining

- L'utilizzo di risorse digitali sulla blockchain per rappresentare valute personalizzate e strumenti finanziari
- storage decentralizzato
- assets non fungibili, quali nomi di dominio ("Namecoin")
- derivati finanziari
- il gioco d'azzardo peer-to-peer
- il sistema di identità e di reputazione sulla blockchain.

Non ci sono quindi solo i "contratti intelligenti" – sistemi che trasferiscono automaticamente assets digitali, in accordo con regole pre-impostate. Quello che Ethereum intende garantire "è una blockchain con una linguaggio di programmazione completo e costruito al suo interno, che può essere usato per creare contratti e per codificare le funzioni arbitrarie di transizione, permettendo agli utenti di creare uno dei sistemi sopra descritti, così come molti altri che ancora non abbiamo immaginato, semplicemente scrivendo la logica in poche righe di codice".

Bibliografia

- Wikipedia
- Blockchain.info
- BTCserv.net
- Coindesk.com