Francesca Failoni
Chief Financial Officer

Alps Blockchain

Il ruolo della blockchain

Tra innovazione digitale e sostenibilità ambientale

About Alps Blockchain

MISSION: costruire un ponte tra la tecnologia della blockchain e il mondo delle fonti rinnovabili, per rendere l'attività di mining sostenibile e valorizzare l'energia green del nostro territorio.

INNOVAZIONE DIGITALE

RICERCA E SVILUPPO

SOSTENIBILITÀ

Cos'è la blockchain

La blockchain è una struttura dati condivisa e immutabile, definita come **registro digitale distribuito** (DLT).

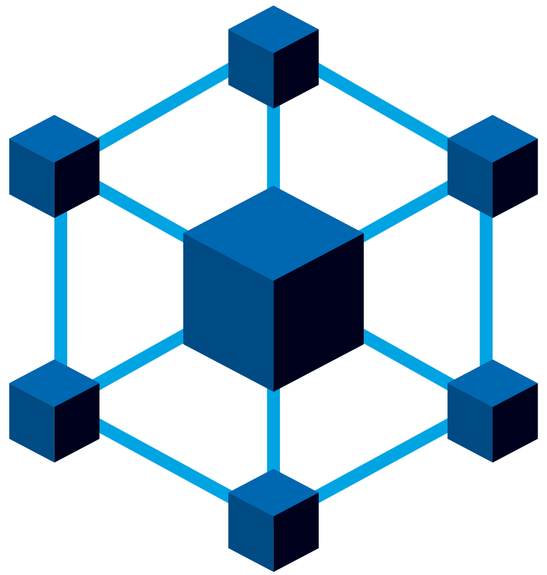
Nella blockchain i blocchi sono collegati in un unico registro, ordinato in ordine cronologico, la cui integrità è garantita dalla **crittografia**.

Come funziona la blockchain

I **blocchi**, che raggruppano le transazioni, vengono elaborati da un **nodo validatore**.

Questo è scelto in modo casuale e confermato dagli altri nodi attraverso un **meccanismo di consenso distribuito** su tutta la rete.

Tali sistemi formano una rete **peer-to-peer** e lavorano insieme per garantire la sicurezza della blockchain



Quali innovazioni introduce

SCARSITÀ DIGITALE

Bitcoin è scarso come l'oro ma può essere inviato facilmente.

UNICITÀ DIGITALE

La blockchain garantisce l'unicità degli asset digitali

IMMUTABILITÀ DEL DATO

I dati contenuti nella blockchain non sono modificabili, a garanzia dell'integrità delle informazioni;

Cos'è il mining

Il mining è il processo che consente di controllare, validare e crittografare un blocco di transazioni in blockchain. In cambio di questa attività si viene remunerati in criptovalute.

BLOCCO

Summary

Height	630,349	Version	0x2000e000	Block Hash	000000000000000000081127aa3ea514305dd7393b22653cb49c7071529ded3c
Confirmations	2	Difficulty	34.89 T / 16.10 T	Prev Block	00000000000000000002009f94e476fe743b9d8447d56a231fef7e4743031bc5
Size	1,300,290 Bytes	Bits	0x17117a39	Next Block	000000000000000000106054f86d6943ef756c75e3455a1082dbaa9103771da9
Stripped Size	897,684 Bytes	Nonce	0x67273a26	Merkle Root	c86000a457440049d1d7b607370047a2b3bf04e338e61628cf301181be630860
Weight	3,993,342	Relayed By	BTC.com		
Tx Count	2,783	Time	2020-05-14 17:13:01	Other Explorers	BLOCKCHAIR

TRANSAZIONE

b50dab5538c7e4a7c673b649a40afc506948e985ec3af2dfa500f7607c01d80b — 966 Satoshis/vByte — 0.00131433 BTC — 2020-05-14 17:13:01

38nPsmzyiXL3nNGa7P6gwmxzpQQytrbafi	0.21810016	1JkbtV85BfpcLsmefwXupVD1qEErmpaaJ5	0.21678583

0.21678583

PROOF OF WORK

Meccanismo di consenso distribuito che prevede la **risoluzione di problemi matematici estremamente complessi che sono inseriti nei blocchi**. La risoluzione restituisce un hash (codice) facilmente verificabile dai nodi della rete.

PROOF OF STAKE

Meccanismo di consenso distribuito in cui i blocchi vengono validati dai nodi della rete in modo **proporzionale al quantitativo di criptovaluta in possesso di quel nodo** (staking), con una distribuzione di probabilità casuale.

Problema del consenso

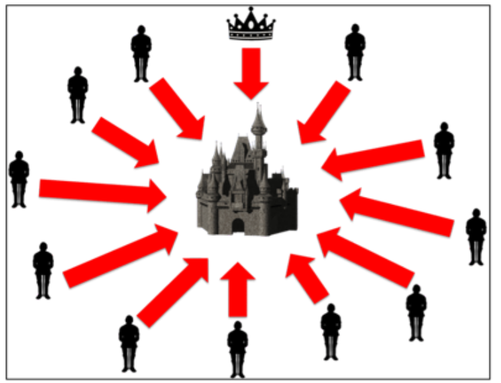
«The Byzantine Generals Problems», Leslie Lamport ,1982

Ciascun generale deve decidere se attaccare o ripiegare e lo scopo è raggiungere il consenso

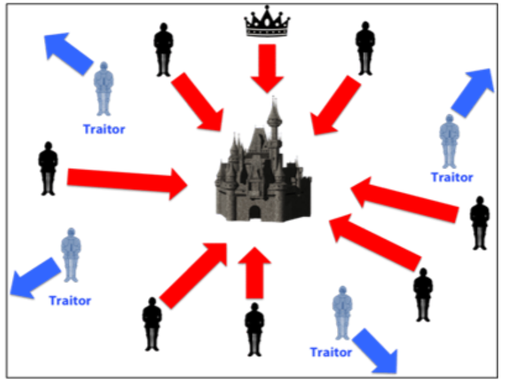
- Una volta presa la decisione, non può essere cambiata;
- Tutti i generali devono concordare sulla stessa decisione ed eseguirla in modo sincronizzato.

Possibili problemi:

- Possono agire in modo disonesto e inviare un messaggio falso;
- I messaggi possono arrivare in ritardo, essere distrutti o smarriti.



Coordinated Attack Leading to Victory



Uncoordinated Attack Leading to Defeat

Problema del consenso

«The Byzantine Generals Problems», Leslie Lamport ,1982

Blockchain (BTC)

Servono ⅔ o più nodi affidabili e onesti. Se la maggioranza del network decide di agire in modo disonesto, il sistema è suscettibile a errori e attacchi, come il 51% attack.

SOLUZIONE:

Algoritmo di consenso PoW. Non è BFT al 100%, ma grazie al costoso processo di mining e alle sottostanti tecniche crittografiche, la PoW si è dimostrata una delle implementazioni più sicure e affidabili per i network blockchain.

PROBLEMA DELLA SIBILLA

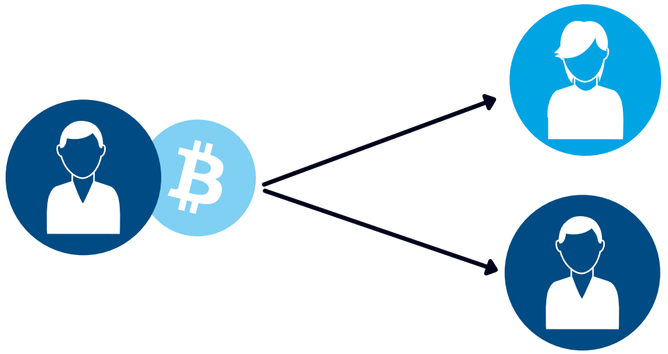
- I nodi onesti di un network possono diventare una minoranza creando sufficienti identità false (o identità Sybil).
- 51% attack: viene cambiato l'ordine delle transazioni e impedita la conferma delle stesse, portando al double spending.

SOLUZIONE

Attraverso l'algoritmo di consenso PoW si rendono gli eventuali attacchi molto costosi: l'abilità di creare un blocco deve essere proporzionale alla potenza di calcolo totale, quindi bisogna possedere effettivamente la potenza di calcolo necessaria per creare un nuovo blocco.

DOUBLE SPENDING

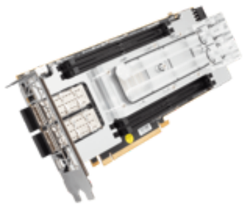
Problema che si verifica nel caso in cui è possibile di spendere più volte lo stesso token.



SOLUZIONE

Gli utenti di bitcoin si proteggono aspettando conferme quando ricevono pagamenti sulla blockchain, le transazioni diventano sempre più irreversibili all'aumentare del numero di conferme. L'unico modo per fare double spending diventa così un attacco al 51%, che sarebbe troppo costoso.

Tecnologie per il mining a confronto



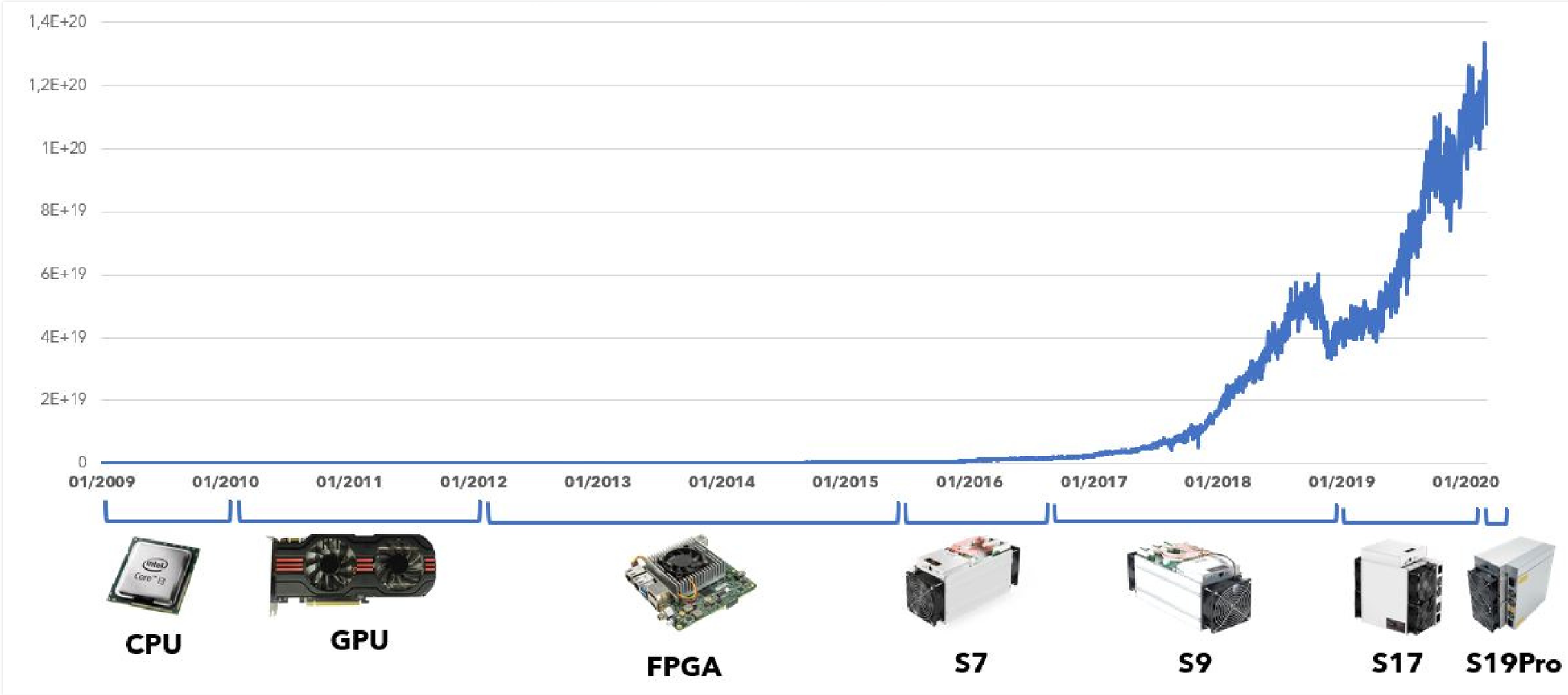
FPGA
field-programmable gate array

ASIC
application specific integrated circuit

GPU
graphics processing unit

Vantaggio	FPGA	ASIC	GPU
Performance	Medie	Alte	Basse
Programmabile	✓	✗	✓
Consumo energetico	Basso	Alto	Medio
Specificità	Vari Algoritmi	Unico Algoritmo	Molti Algoritmi
Obsolescenza	Bassa	Alta	Media
Rivendibilità	Bassa	Media	Alta

Tecnologie per il mining - Hashrate (Hash/s) Totale Bitcoin



Aspetti tecnici

HASHRATE

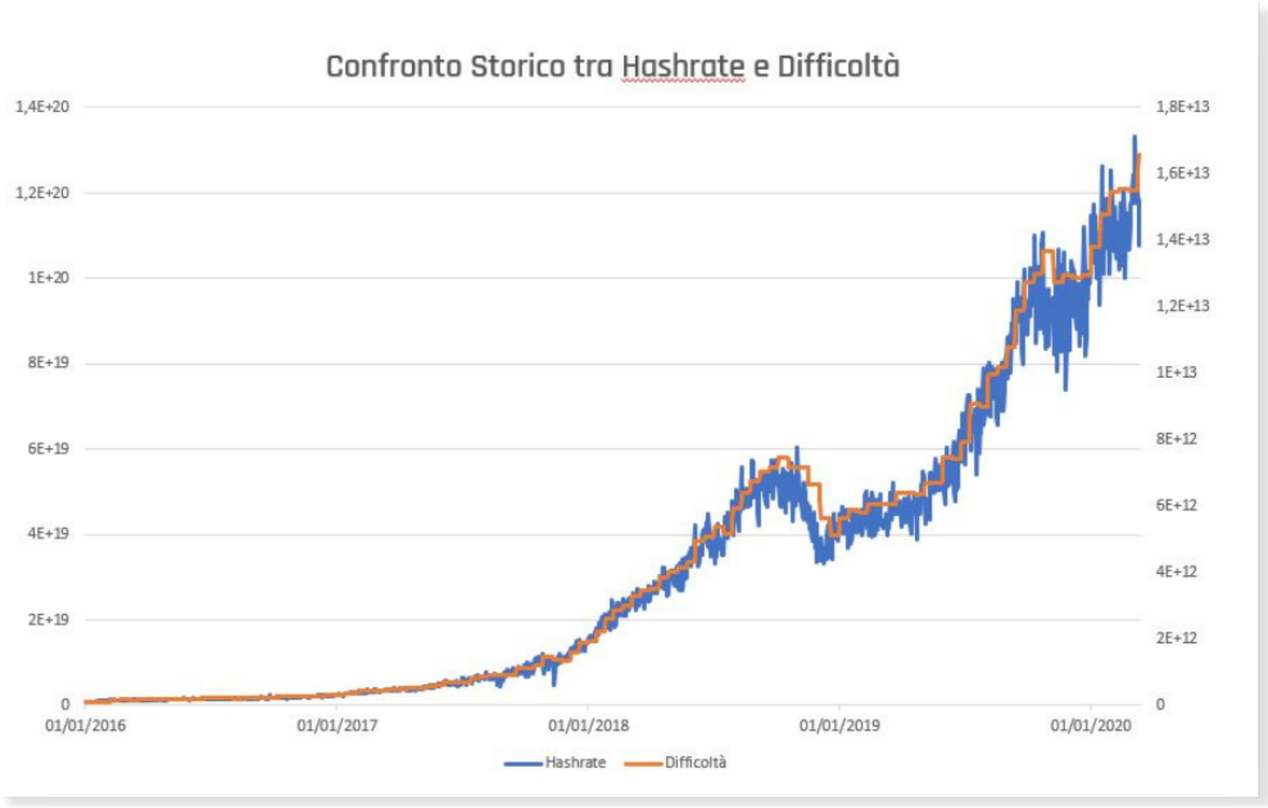
potenza computazionale immessa nella Blockchain di Bitcoin, misurata in hash; dipende da quanti miner sono collegati alla rete;

DIFFICOLTÀ

potenza computazionale necessaria per risolvere il problema crittografico incluso nel blocco; la difficoltà della rete si aggiorna ogni 2.016 blocchi, ogni 14 giorni ca;

HALVING

eventi in cui la generazione di nuova criptovaluta (bitcoin) viene dimezzata, programmati per accadere ogni 210.000 blocchi confermati, fino a che i Bitcoin raggiungeranno l'offerta totale programmata pari a 21.000.000, nel 2140 ca.



La blockchain è una tecnologia ad alta intensità energetica, tuttavia stiamo vivendo la rivoluzione della tecnologia dei dati e anche i dati consumano molta energia.

Abbiamo una scelta: combattere il cambiamento tecnologico o cercare di renderlo più sostenibile.

Mining e consumo energetico nel mondo

154.620 TWh

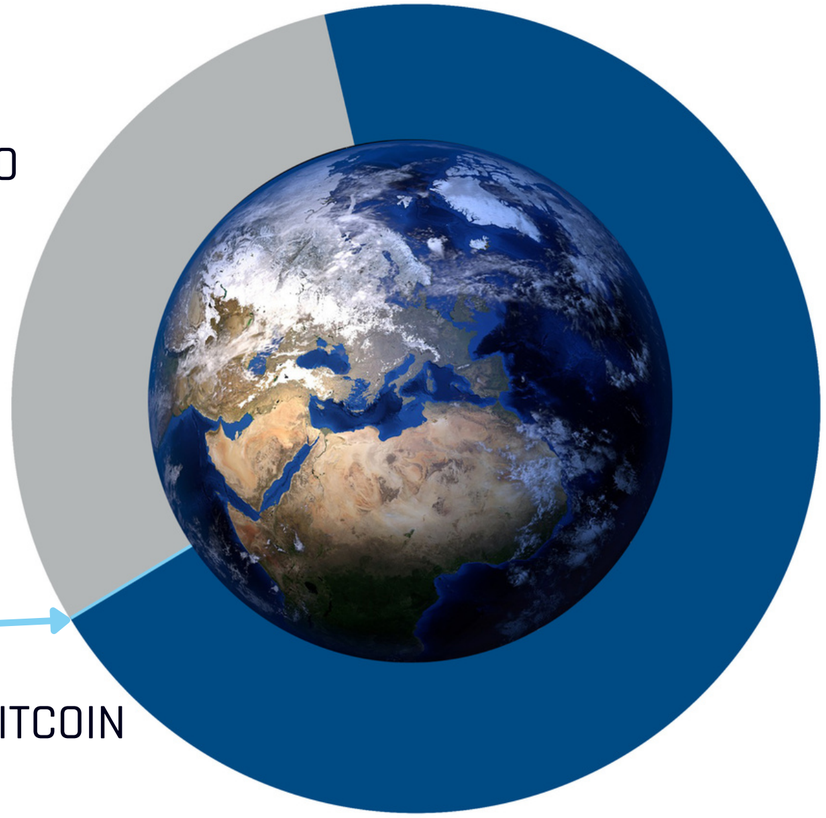
ENERGIA TOTALE GENERATA NEL MONDO

50.000 TWh

ENERGIA PERSA PER INEFFICIENZE

188 TWh

ENERGIA CONSUMATA DAL MINING DI BITCOIN



Consumo mondiale nel mining di bitcoin

0,12%

della produziona energetica mondiale

0,38%

dell'energia mondiale sprecata

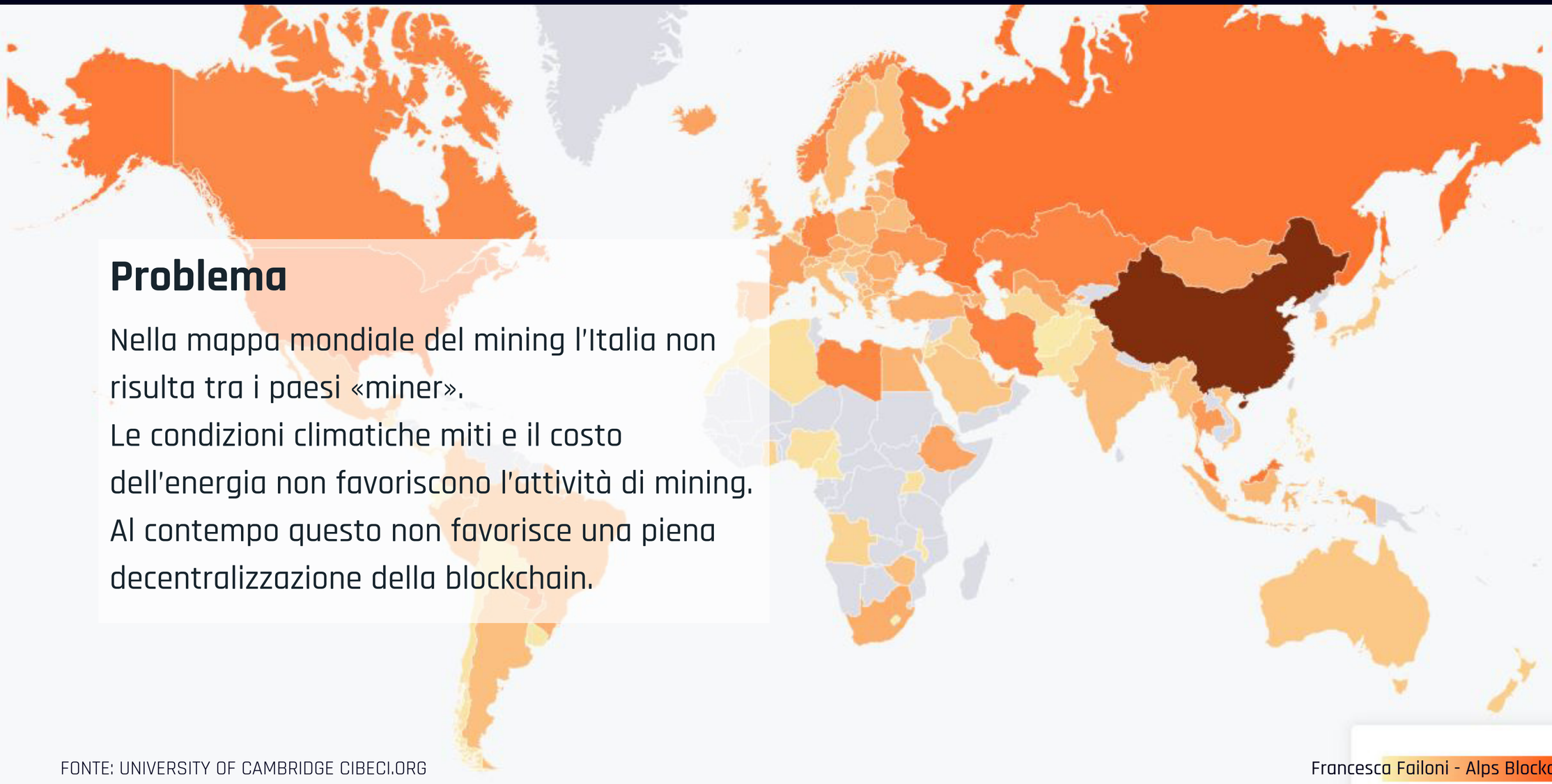
FONTE: BITCOIN MINING COUNCIL, stime settembre 2021

Francesca Failoni - Alps Blockchain Srl

Mining in Italia

Problema

Nella mappa mondiale del mining l'Italia non risulta tra i paesi «miner».
Le condizioni climatiche miti e il costo dell'energia non favoriscono l'attività di mining.
Al contempo questo non favorisce una piena decentralizzazione della blockchain.



FONTE: UNIVERSITY OF CAMBRIDGE CIBECI.ORG

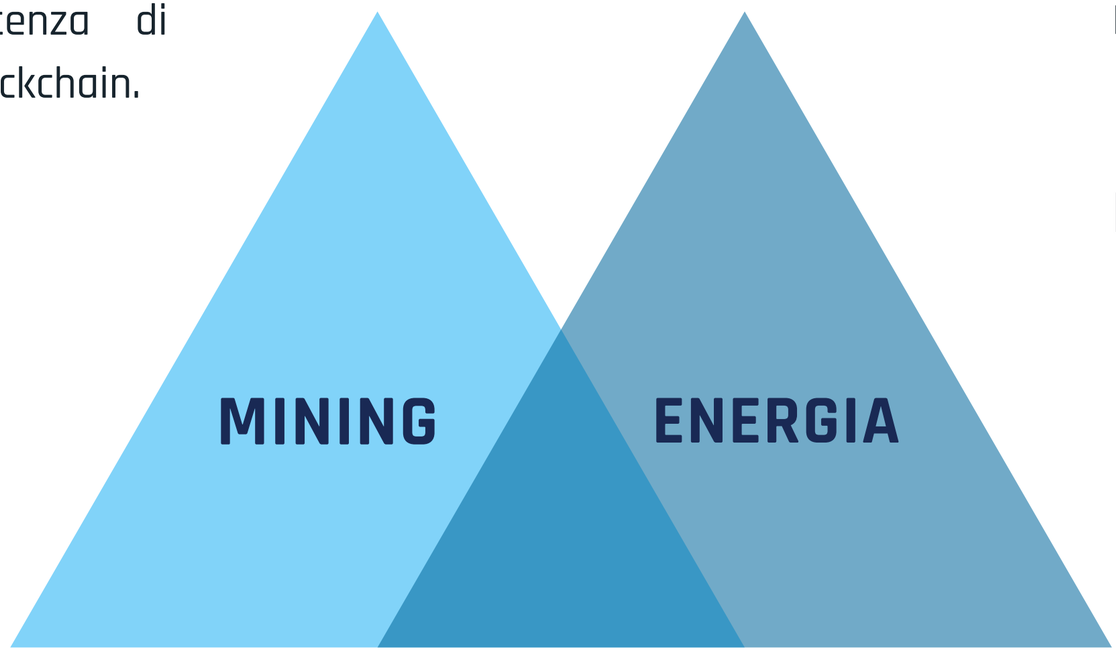
Mining e consumo energetico in Italia

Opportunità

Bisogno di maggiore potenza di calcolo per l'infrastruttura blockchain.

Problema

- Elevato dispendio energetico richiesto dall'attività di mining.
- Costo dell'energia in Italia.
- Sostenibilità della tecnologia.



Opportunità

Energie zero-carbon.

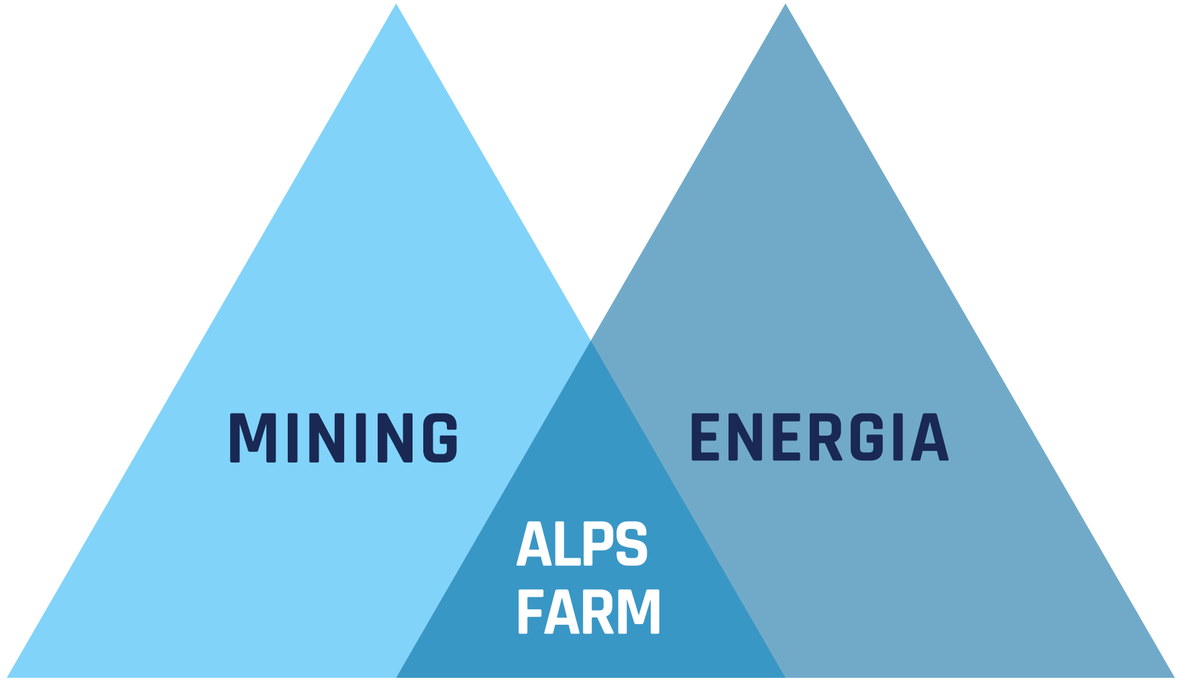
Problema

- Incentivi statali ai produttori di energia rinnovabili in scadenza.
- Settore già maturo.
- Calo PUN

Mining e consumo energetico in Italia

Soluzione

- Autoconsumare l'energia prodotta e fare mining in modo sostenibile.
- Favorire la creazione di mining farm in Italia utilizzando e valorizzando l'energia idroelettrica
- Ottimizzare la tecnologia e gestire i miner in maniera innovativa, grazie a un lavoro di R&S



Alps Farm: dalla potenza dell'acqua alla potenza di calcolo

Alps Farm - 2021

300
PH/S

9
MW

18 MINING FARM IN ITALIA

2.100 MINERS INSTALLATI

100% ENERGIA IDROELETTRICA

Francesca Failoni

Chief Financial Officer
Alps Blockchain Srl

f.failoni@alpsblockchain.com

www.alpsblockchain.com