

Blockchain e Smart contract per giuristi 3.0

Biagio Distefano

HASH

sha256

“siena” ————— **sha256()** —————→ **d01ba29d08682f7dca2b88778c9a62f26
7b8de9e6e7928d68062cddb3e31ab**

“Siena” ————— **sha256()** —————→ **4f0330ebcf315c82899e61e942084d755
8d842d11208f3de55c9ccb10170bd69**

**“Palio di
Siena”** ————— **sha256()** —————→ **7e010733a266c2ce7e63f03c6d3e74e08
8eac1b594dc47d7e0caa50d696dec26**



————— **sha256()** —————→ **bfd1e56aba2696014c123bc8912663a0
1a758081a921632ff6571505f52e33dd**

Caratteristiche dell'HASH

- **Deterministico:** gli stessi bit in input daranno sempre lo stesso output
- **Dimensione fissa:** indipendentemente dall'input, l'output avrà sempre la stessa dimensione
- **Unidirezionale:** non è possibile ricavare l'input dall'output

Provate su

<https://anders.com/blockchain/hash.html>

Mettiamo i dati in un Blocco

N. Blocco	1
Nonce	30306
Dati	Ciao, Siena!
HASH	0000b3169547f3012b53026af434b84c9c83ecef64c0aeecbf63d38302caf8f4

Validità del Blocco

Mining

- Nel nostro esempio, per essere valido, il blocco deve avere un hash che inizia con **0000**
- Per validare il blocco, cambiamo il valore del **Nonce** e ricalcoliamo l'hash fin quando non inizia con **0000**
- Questa operazione, detta **Mining**, è estremamente complessa e computazionalmente costosa

Provate su

<https://anders.com/blockchain/block.html>

Concateniamo più Blocchi

#Blocco	1	#Blocco	2	#Blocco	3
Nonce	30306	Nonce	44329	Nonce	11447
Dati	Ciao, Siena!	Dati	Oggi sei più smart!	Dati	Che bella la blockchain!
HASH prev	00000000000000000000000000000000	HASH prev	00007721391f93cf1fd3c061ad117e0ad3cdd4b9a7a0c4	HASH prev	00002f913be209a8c449dfc378fbb2516a7b5329cf5936d
HASH	00007721391f93cf1fd3c061ad117e0ad3cdd4b9a7a0c4	HASH	00002f913be209a8c449dfc378fbb2516a7b5329cf5936d	HASH	000084db93c8ff3fa84e2f4076611d2488c3977001db40

Provate su

<https://anders.com/blockchain/blockchain.html>

Dove si trova la blockchain, fisicamente?

- Non c'è un server centrale
- Non c'è un'Autorità che controlla
- Chiunque può partecipare come “Nodo”
- Ogni nodo (peer) ha una copia integrale della blockchain
- Per questo si chiama Registro Distribuito (DLT: Distributed Ledger Technology)

Registri distribuiti

Nodo di Tizio

#Blocco	1
Nonce	30306
Dati	Ciao, Siena!
HASH prev	00000000000000000000000000000000 00000000000000000000000000000000
HASH	00007721391f93cf1fd3c061 ad117e0ad3cdd4b9a7a0c4



#Blocco	2
Nonce	44329
Dati	Oggi sei più smart!
HASH prev	00007721391f93cf1fd3c061 ad117e0ad3cdd4b9a7a0c4
HASH	00002f913be209a8c449dfc3 78fbb2516a7b5329cf5936d



#Blocco	3
Nonce	11447
Dati	Che bella la blockchain!
HASH prev	00002f913be209a8c449dfc3 78fbb2516a7b5329cf5936d
HASH	000084db93c8ff3fa84e2f40 76611d2488c3977001db40

Nodo di Caio

#Blocco	1
Nonce	30306
Dati	Ciao, Siena!
HASH prev	00000000000000000000000000000000 00000000000000000000000000000000
HASH	00007721391f93cf1fd3c061 ad117e0ad3cdd4b9a7a0c4



#Blocco	2
Nonce	44329
Dati	Oggi sei più smart!
HASH prev	00007721391f93cf1fd3c061 ad117e0ad3cdd4b9a7a0c4
HASH	00002f913be209a8c449dfc3 78fbb2516a7b5329cf5936d



#Blocco	3
Nonce	11447
Dati	Che bella la blockchain!
HASH prev	00002f913be209a8c449dfc3 78fbb2516a7b5329cf5936d
HASH	000084db93c8ff3fa84e2f40 76611d2488c3977001db40

Provate su

<https://anders.com/blockchain/distributed.html>

Ok, ma i Bitcoin?

Dati strutturati!

#Blocco	1		
Nonce	11622		
Transazioni	Da	A	₿
1	Tizio	Caio	10
2	Sempronio	Mevio	5
3	Filano	Calpurnio	3
4	Caio	Sempronio	1
5	Calpurnio	Mevio	6
HASH prev	000 000000000000		
HASH	0000 a36214cf88221c68011fe76215146268f8ea3a4a5db80335b9 0e12e80363		

Provate su

<https://anders.com/blockchain/tokens.html>

Le transazioni in BTC

- “Tizio manda a Caio 1 BTC”
- Questa transazione viene comunicata a tutta la rete Bitcoin (ossia ai nodi, cd *peers*)
- Le transazioni vengono raggruppate per creare un blocco
- Il blocco viene validato (minato)
- Il nodo-minatore che per primo valida il blocco (c.d. **Proof of Work - PoW**) ha il diritto di inserirlo nella blockchain e viene ricompensato in BTC

La sicurezza delle transazioni

- “Tizio manda a Caio 1 BTC” —————> Come accertarlo?

Crittografia Asimmetrica

Crittografia Asimmetrica

Chiavi pubbliche e private

- **Chiave privata**
 - Deve essere tenuta segreta
 - Viene usata per criptare un documento (o qualsiasi dato)
- **Chiave pubblica**
 - Deriva unidirezionalmente dalla chiave privata (provate su <https://anders.com/blockchain/public-private-keys/keys.html>)
 - Va comunicata ai destinatari
 - Viene usata per decriptare il documento (o qualsiasi dato) criptato con la chiave privata corrispondente

Firma Digitale

- **Per firmare digitalmente un documento (o una transazione BTC):**
 - Genero l'hash del documento
 - Cripto l'hash con la chiave privata
- **Per verificare la genuinità della firma:**
 - Decripto l'hash criptato con la chiave pubblica
 - Genero l'hash del documento
 - Verifico che l'hash del documento e l'hash decrittato coincidano

Private su

<https://anders.com/blockchain/public-private-keys/signatures.html>

Indirizzi Bitcoin

Nella blockchain Bitcoin (e in tutte le altre) non avremo “Tizio” e “Caio” ma indirizzi di portafogli che derivano dalle chiavi pubbliche

1FeexV6bAHb8ybZjqQMjJrcCrHGW9sb6uF

Private su

[https://anders.com/blockchain/public-private-keys/
transaction.html](https://anders.com/blockchain/public-private-keys/transaction.html)

E

[https://anders.com/blockchain/public-private-keys/
blockchain.html](https://anders.com/blockchain/public-private-keys/blockchain.html)

Interagiamo con la blockchain Ethereum



Installate MetaMask

<https://metamask.io/>

(Firefox, Chrome o Opera)

Esplorate la blockchain su Etherscan

Rete Principale: <https://etherscan.io/>

Rete di prova Ropsten: <https://ropsten.etherscan.io/>

Accedete alla Chat

[https://tlk.io/
smartsiena](https://tlk.io/smartsiena)