D.Marazzina

Blockchain: an introduction

9 Maggio 2018

DLT=Distributed Ledger Technology

Distributed Ledger = Registro (Database) Distribuito gestito da una rete peer to peer attraverso dei meccanismi di consenso che consentono l'assenza di fiducia fra i nodi.

In un database distribuito generalmente vi è fiducia fra i nodi della rete. Nel caso di Bitcoin, non vi è fiducia e per questo si utilizzano dei meccanismi di consenso.

Blockchain è un tipo di Database Distribuito, costruito su blocchi concatenati

BITCOIN E BLOCKCHAIN…
Tutto parte da qui

Bitcoin

Bitcoin è una moneta elettronica creata nel 2009, il cui inventore è noto con lo pseudonimo Satoshi Nakamoto

E' una delle prime implementazioni di criptovaluta: una valuta decentralizzata digitale che si basa sui principi della crittografia per convalidare le transazioni e per la generazione di moneta.

Keywords:
decentralizzata
crittografia
generazione di moneta

Keywords 1: Decentralizzata

- Politicamente decentralizzato: Bitcoin non è controllato da un'entità specifica.
- Architetturalmente decentralizzato (o distribuito): Bitcoin vive su macchine distribuite sull'intero pianeta.
- Logicamente centralizzato: tutte le macchine su cui vive Bitcoin sono d'accordo su uno stato condiviso (e.g. quanti bitcoin ha ognuno).

Una blockchain è un database distribuito (o architetturalmente decentralizzato) e politicamente decentralizzato gestito da una rete peer to peer attraverso dei meccanismi di consenso distribuito (al fine di accordarsi su uno stato condiviso, in quanto logicamente centralizzato).

Keywords 1: Decentralizzata → Blockchain

Bitcoin non fa uso di un ente centrale, come una banca centrale, per la gestione delle transazioni e la creazione di moneta: esso utilizza un database distribuito tra i nodi della rete che tengono traccia delle transazioni

Database Distribuito:
gli archivi **di dati (come lo storico delle transazioni) non sono memorizzati in un solo computer o server, bensì su più computer o server, detti nodi.**
Il database in senso fisico è distribuito su una rete di computer connessi tra loro via internet. Tutti i computer memorizzano tutto il database.

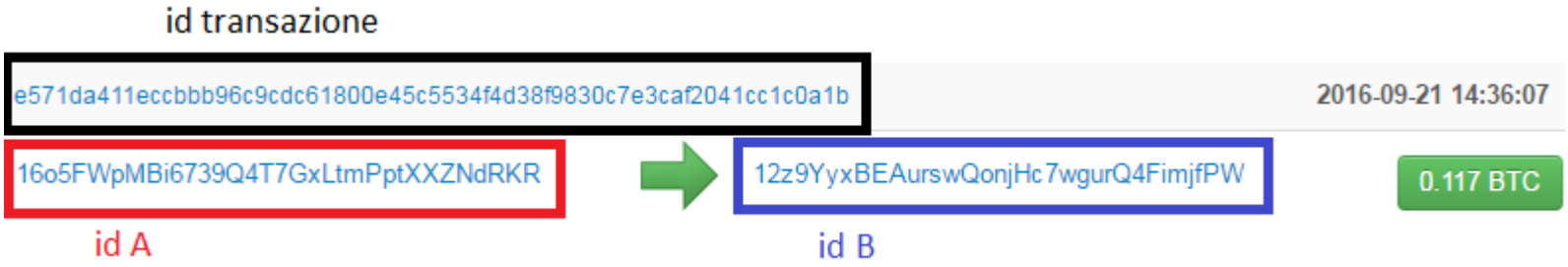
Questo database distribuito è la cosiddetta Blockchain. La Blockchain è la tecnologia su cui agisce la diffusione di Bitcoin, è come un DNA che rappresenta lo storico delle operazioni finanziarie. Chiunque può farne parte: basta installare un software.

Ma come funziona Blockchain?
Cominciamo dall' ABC (https://bitcoin.org/it/glossario)

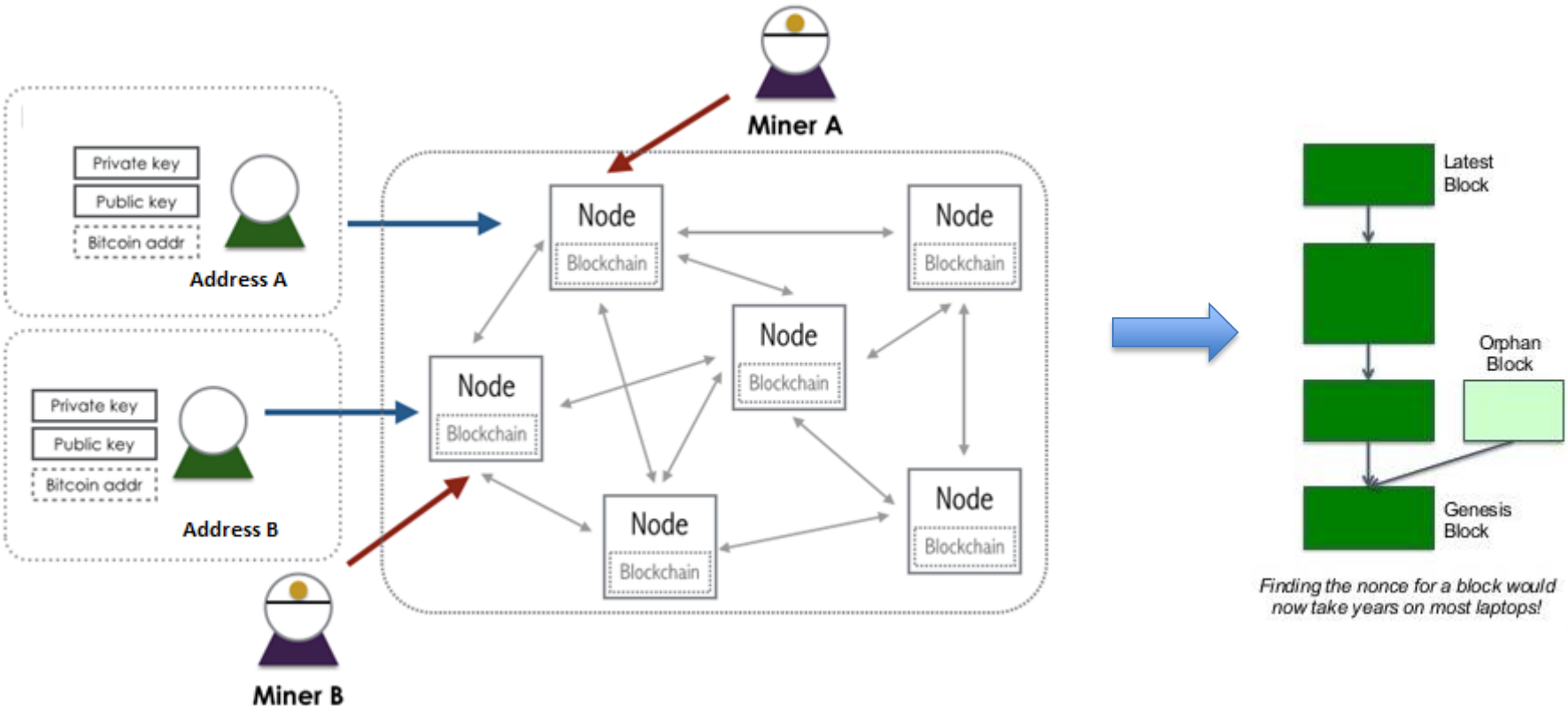
- Transazione: Una transazione è un trasferimento di Bitcoin che viene incluso nella Blockchain. Una transazione è identificata dai due *address* (controparti) e dall'ammontare scambiato.

  La firma crittografica a chiave privata delle due controparti fornisce una prova della loro identità e che i Bitcoin provengano dal reale proprietario. La firma impedisce anche che la transazione (una volta eseguita) venga alterata da altri.

  I due address sono identificati pubblicamente tramite un codice.



Ma come funziona Blockchain?



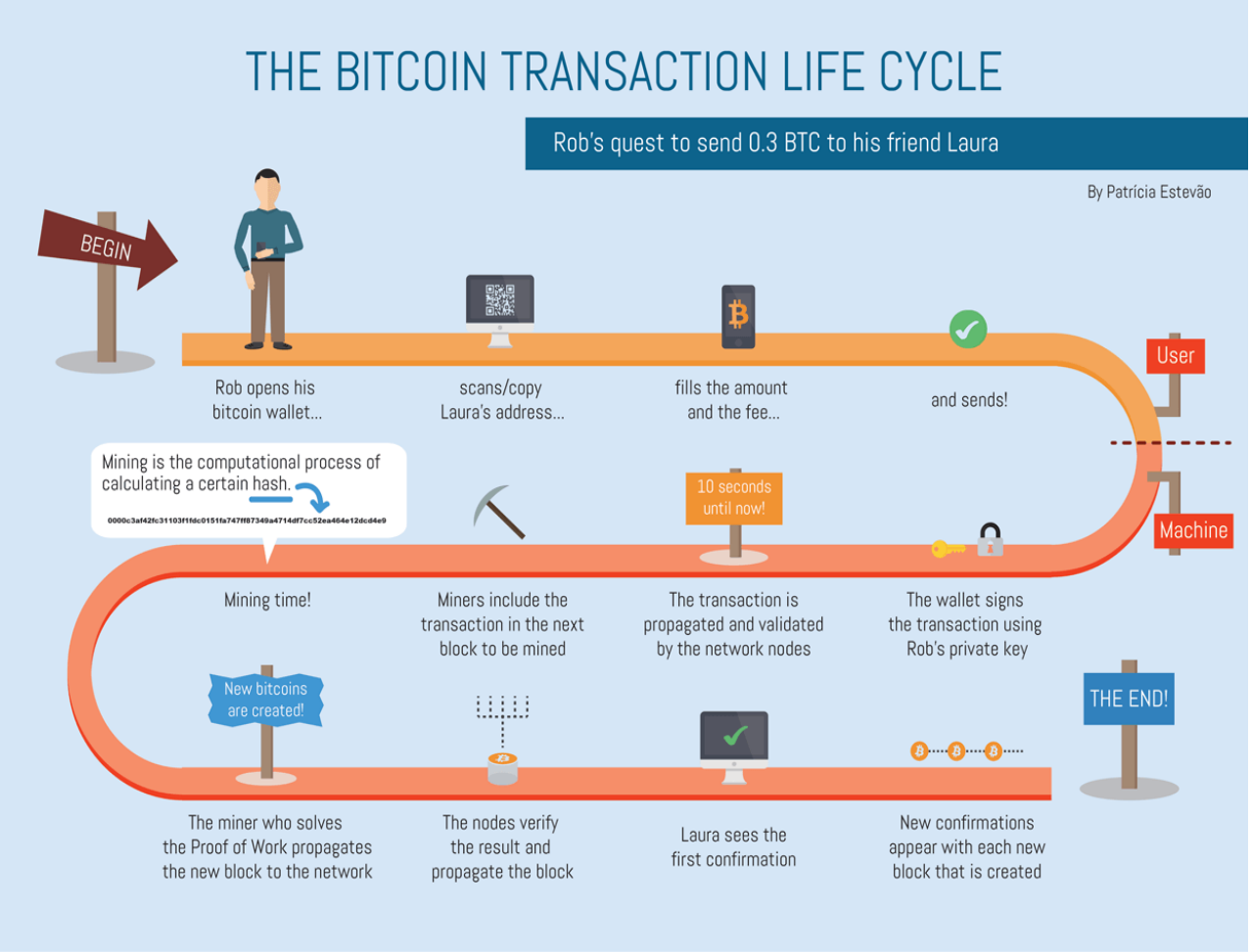
Ma come funziona Blockchain?

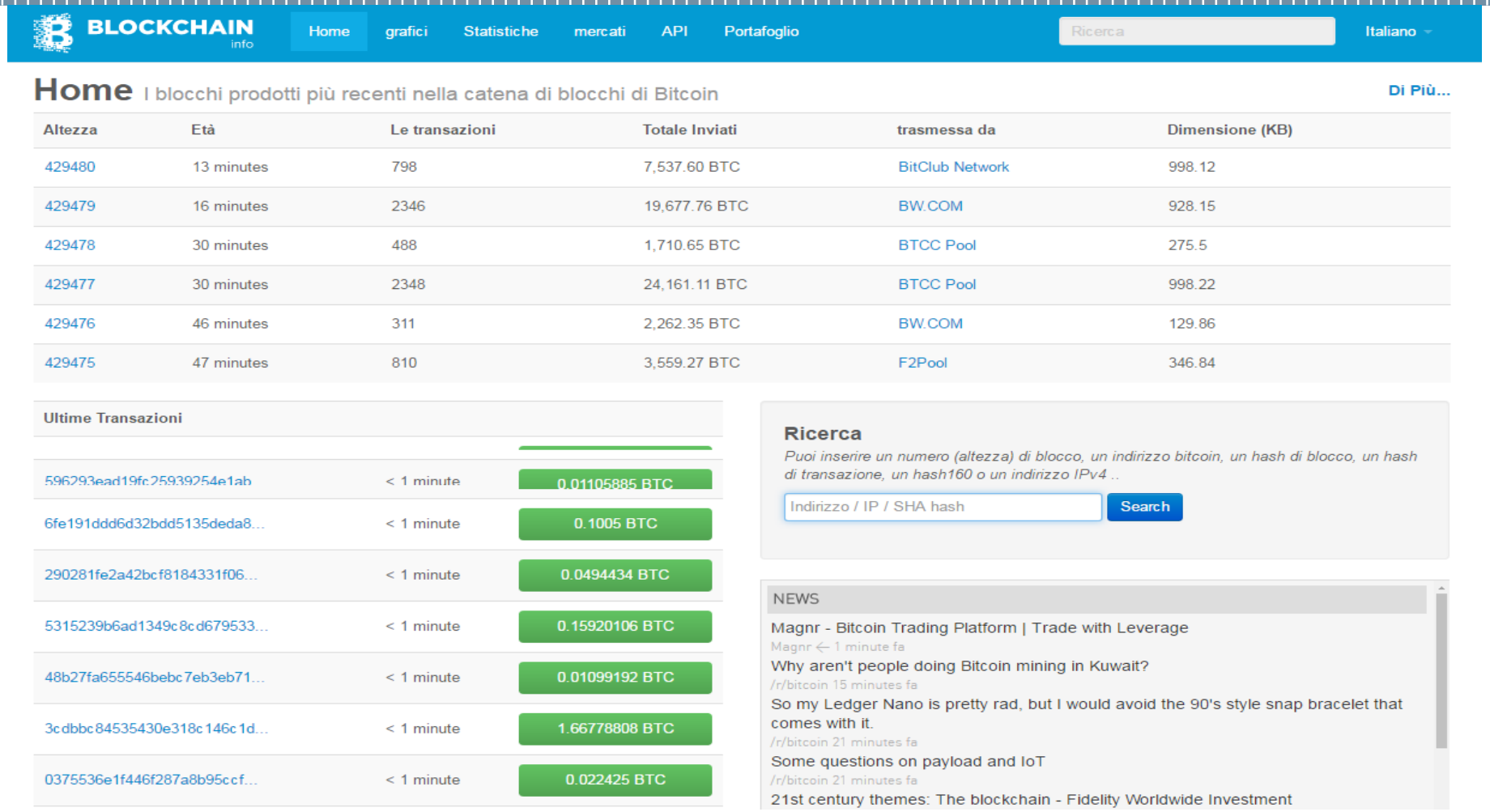
- Blocco: un blocco è una parte della Blockchain che contiene una serie di transazioni (di Bitcoin). In media, un nuovo blocco, che include delle transazioni, viene aggiunto alla Blockchain ogni dieci minuti.
- Conferma: per essere inclusa in un blocco, e quindi nella Blockchain, una transazione deve essere confermata da più nodi (*miners*), cioè a dire processata dalla rete.
- Mining: è un processo matematico eseguito dai nodi della Blockchain sul blocco candidato, una volta risolto il quale il blocco (e quindi tutte le transazioni registrate in esso) viene confermata e inserita in un blocco della Blockchain. Come ricompensa per il loro servizio, i *miners* (minatori) possono incassare nuovi Bitcoin appena creati.

Essenzialmente i miner accumulano transazioni in continuazione (selezionandole con un certo criterio, come quelle che offrono le fee più alte).

Quando hanno transazioni a sufficienza per riempiere un blocco (che ha una dimensione fissata) provano a risolvere il problema di mining.

Il primo miner che risolve il problema di mining propaga il blocco nella rete, il quale viene verificato (verificano se la proof of work è valida) dagli altri nodi e aggiunto alla loro copia della blockchain.


THE BITCOIN TRANSACTION LIFE CYCLE
Rob's quest to send 0.3 BTC to his friend Laura
By Patrícia Estevão
BEGIN
Rob opens his bitcoin wallet...
scans/copy Laura's address...
fills the amount and the fee...
and sends!
User
Machine
Mining is the computational process of calculating a certain hash.
0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
10 seconds until now!
Mining time!
Miners include the transaction in the next block to be mined
The transaction is propagated and validated by the network nodes
The wallet signs the transaction using Rob's private key
New bitcoins are created!
THE END!
The miner who solves the Proof of Work propagates the new block to the network
The nodes verify the result and propagate the block
Laura sees the first confirmation
New confirmations appear with each new block that is created


BLOCKCHAIN info
Home
grafici
Statistiche
mercati
API
Portafoglio
Ricerca
Italiano
Home I blocchi prodotti più recenti nella catena di blocchi di Bitcoin
Di Più...
Altezza | Età | Le transazioni | Totale Inviati | trasmessa da | Dimensione (KB)
429480 | 13 minutes | 798 | 7,537.60 BTC | BitClub Network | 998.12
429479 | 16 minutes | 2346 | 19,677.76 BTC | BW.COM | 928.15
429478 | 30 minutes | 488 | 1,710.65 BTC | BTCC Pool | 275.5
429477 | 30 minutes | 2348 | 24,161.11 BTC | BTCC Pool | 998.22
429476 | 46 minutes | 311 | 2,262.35 BTC | BW.COM | 129.86
429475 | 47 minutes | 810 | 3,559.27 BTC | F2Pool | 346.84
Ultime Transazioni
596293ead19fc25939254e1ab | < 1 minute | 0.01105885 BTC
6fe191ddd6d32bdd5135deda8... | < 1 minute | 0.1005 BTC
290281fe2a42bcf8184331f06... | < 1 minute | 0.0494434 BTC
5315239b6ad1349c8cd679533... | < 1 minute | 0.15920106 BTC
48b27fa655546bebc7eb3eb71... | < 1 minute | 0.01099192 BTC
3cdbbc84535430e318c146c1d... | < 1 minute | 1.66778808 BTC
0375536e1f446f287a8b95ccf... | < 1 minute | 0.022425 BTC
Ricerca
Puoi inserire un numero (altezza) di blocco, un indirizzo bitcoin, un hash di blocco, un hash di transazione, un hash160 o un indirizzo IPv4 ..
Indirizzo / IP / SHA hash
Search
NEWS
Magnr - Bitcoin Trading Platform | Trade with Leverage
Magnr ← 1 minute fa
Why aren't people doing Bitcoin mining in Kuwait?
/r/bitcoin 15 minutes fa
So my Ledger Nano is pretty rad, but I would avoid the 90's style snap bracelet that comes with it.
/r/bitcoin 21 minutes fa
Some questions on payload and IoT
/r/bitcoin 21 minutes fa
21st century themes: The blockchain - Fidelity Worldwide Investment

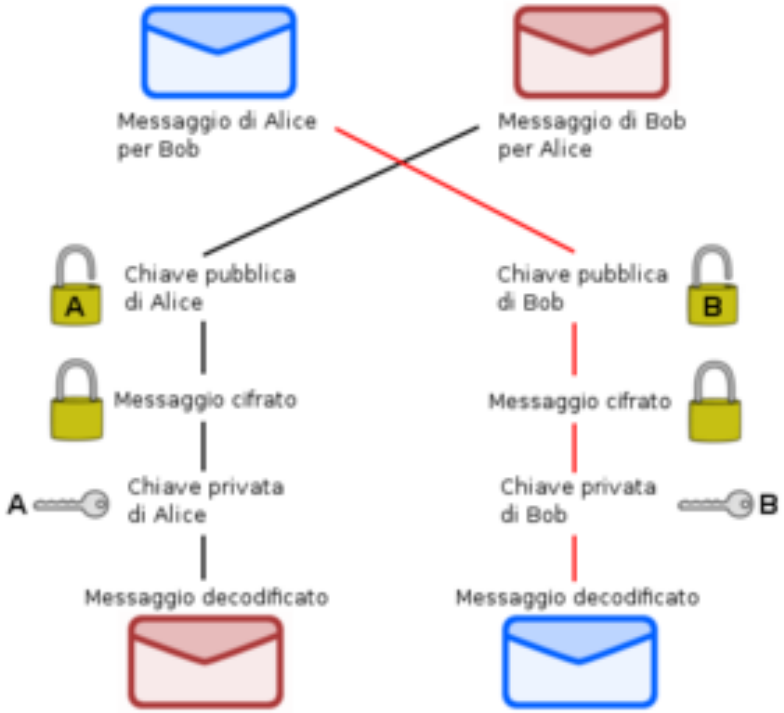
Keywords 2: crittografia

- Firma criptografica: è un meccanismo matematico che consente di provare l'identità e la proprietà in questo caso dei Bitcoin.

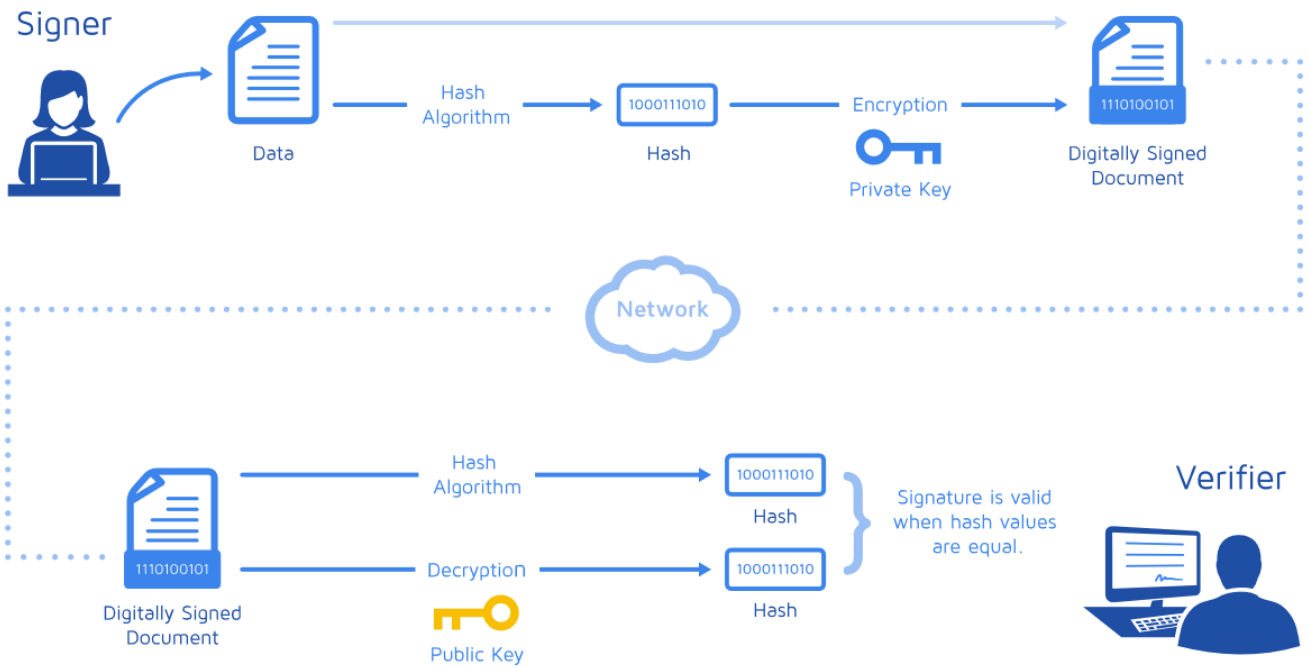
Quando il tuo software Bitcoin segna una transazione con la tua chiave privata, l'intera rete può riconoscerti (non come persona fisica ma come id) e verificare che i Bitcoin spesi siano in tuo possesso. La transazione diviene di pubblico dominio rispetto al tuo codice.

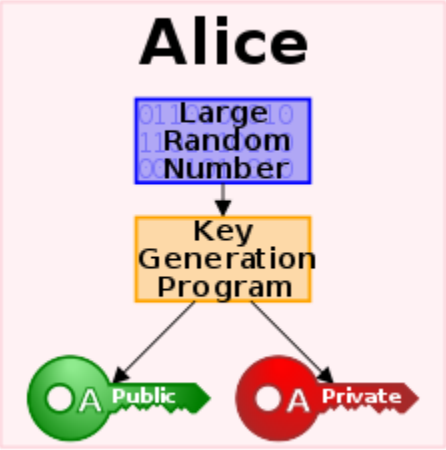
Ad oggi non c'è alcun modo per gli altri nodi d'indovinare la tua chiave privata, per derubarti dei tuoi Bitcoin.

Crittografia asimmetrica (o a chiave pubblica)

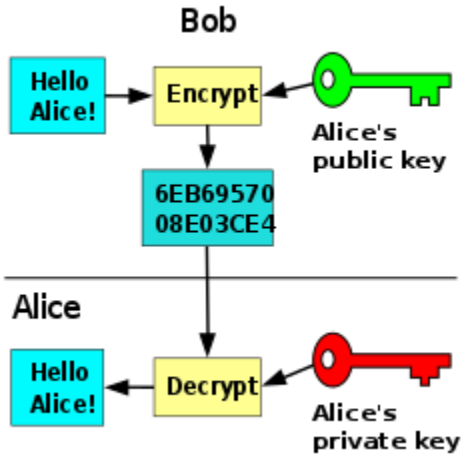


Firma digitale





Step 1: viene generata una coppia chiave pubblica – privata per Alice



Step 2: Bob usa la chiave pubblica di Alice per criptare il messaggio. Solo chi ha la chiave privata di Alice può decriptarlo!

Quindi, se Alice ha tenuta nascosta la chiave privata, solo lei può leggere il messaggio

Crittografia Ellittica

Fra le crittografie asimmetriche, Bitcoin usa la Crittografia Ellittica

Le chiavi pubbliche si basano sulla creazione di un problema matematico molto difficile da risolvere senza informazioni, ma che con l'utilizzo di alcune informazioni (la chiave privata) diventa di semplice e rapida risoluzione.
L'utente distribuisce pubblicamente il problema (la chiave pubblica) e tiene nascoste le informazioni aggiuntive (la chiave privata).
Il problema viene utilizzato per mescolare i messaggi da trasmettere in modo da renderli non comprensibili.

Elliptic Curve Digital Signature Algorithm: firma digitale protetta da tale crittografia

Un esempio: crittografia RSA

- Prendiamo due numeri primi, 13 e 7 (e non sveliamoli a nessuno)
- Moltiplichiamoli fra loro: otteniamo n=91
- Scegliamo una chiave pubblica: 5
- Usiamo l'Extended Euclidean Algorithm con input 5, 7 e 13, e otteniamo la chiave privata: 29
- Quindi n=91, chiave pubblica 5, chiave privata 29

Sia noto a Alice e Bob che n=91, la chiave pubblica di Alice sia 5, quella privata 29.

Bob vuole mandare un messaggio ad Alice: il messaggio è «3»

Allora moltiplica per 5 volte 3 per se stesso, modulo 91

3*3=9

9*3=27

27*3=81

81*3=243>91→ 243(91)=61

→ Il messaggio pubblico è 61

```
a=3; at=3;
for i=1:5-1
        at=mod(at*a,91)
end
```

→ Output=61

```
a=61; at=61;
for i=1:29-1
        at=mod(at*a,91)
end
```

→ Output=3 → ABBIAMO DECODIFICATO IL MESSAGGIO

Criptare messaggi

1) Associare ad ogni lettera un numero

A	B	C	D	E	F	G	H	I	J	K	L	M
65	66	67	68	69	70	71	72	73	74	75	76	77
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
78	79	80	81	82	83	84	85	86	87	88	89	90

1) Cloud = 67, 76, 79, 85, 68
2) Criptare Cloud → 58, 20, 53, 50, 87

Sicurezza

- Alice e Bob conoscono n=91
- Tutti conoscono 5
- Solo Alice conosce 29

- La conoscenza di 5 (chiave pubblica) non è sufficiente a decriptare il messaggio
- Bob può risalire alla chiave privata di Alice? Cioè l'informazione «91» è sufficiente per compromettere la sicurezza?

Problema matematico: fattorizzazione in numeri primi

La fattorizzazione in numeri primi non è il problema più difficile su base bit-for-bit. Algoritmi specializzati come il Quadratic Sieve e il General Number Field Sieve sono stati creati per affrontare il problema della fattorizzazione e hanno avuto un discreto successo. Questi algoritmi sono più veloci e meno intensi dal punto di vista computazionale rispetto all'approccio ingenuo di indovinare solo coppie di numeri primi conosciuti.

Questi algoritmi di factoring diventano più efficienti man mano che la dimensione dei numeri presi in considerazione aumenta. Il divario tra la difficoltà di fattorizzazione di grandi numeri e la moltiplicazione di grandi numeri si riduce man mano che il numero (cioè la lunghezza del bit della chiave) aumenta. Man mano che le risorse disponibili per decrittografare i numeri aumentano, la dimensione delle chiavi deve crescere ancora più velocemente. Questa non è una situazione sostenibile per dispositivi mobili e di bassa potenza che hanno una potenza computazionale limitata. Il divario tra factoring e moltiplicazione non è sostenibile a lungo termine.

Tutto ciò significa che RSA non è il sistema ideale per il futuro della crittografia.

→ Tecniche basate su Curve Ellittiche

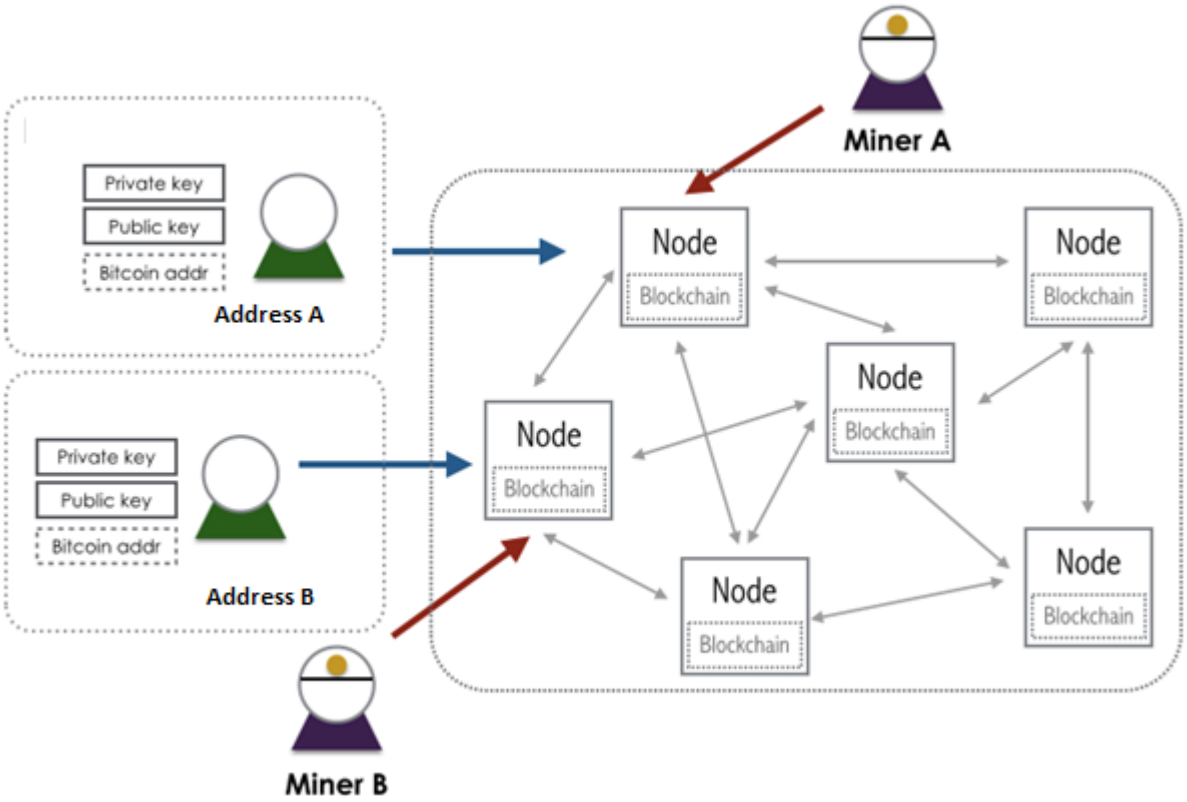
Firma crittografica

Gli algoritmi asimmetrici garantiscono la confidenzialità nella comunicazione. Infatti, un messaggio cifrato con la chiave pubblica del destinatario fa sì che solo quest'ultimo sia in grado di decifrare tale messaggio, in quanto è l'unico che possiede la corrispondente chiave privata.

Inoltre invertendo l'utilizzo delle chiavi, ossia cifrando con la chiave privata del mittente e decifrando con la chiave pubblica del mittente, è possibile garantire l'autenticazione. È su tale principio che si basa la firma digitale.

Il messaggio viene crittografato con la chiave privata, in modo che chiunque possa, utilizzando la chiave pubblica conosciuta da tutti, decifrarlo e, oltre a poterlo leggere in chiaro, essere certo che il messaggio è stato mandato dal possessore della chiave privata corrispondente a quella pubblica utilizzata per leggerlo.

Torniamo alla Blockchain…



E i miners cosa fanno?

Oltre a controllare che le firme digitali delle transazioni siano autentiche, che non avvenga double spending, etc., e quindi verificare la transazione, il loro lavoro principale è quello di costruire la Blockchain, blocco per blocco.

Come?

Concatenando fra loro i blocchi, e questo avviene con la risoluzione di un problema matematico computazionalmente oneroso.

Se fosse facilmente risolvibile, sarebbe anche facile attaccare la Blockchain.

Proof of Work

La Blockchain di Bitcoin si basa quindi sulla proof-of-work

La *Proof of Work*, o PoW, è un algoritmo che viene utilizzato da diverse criptovalute - come Bitcoin e Ethereum- per raggiungere un accordo decentralizzato tra diversi nodi nel processo di aggiunta di un blocco specifico alla blockchain.

Hashcash (SHA-256) è la funzione Proof of Work utilizzata dal Bitcoin. La criptovaluta obbliga i miners a risolvere dei **problemi matematici estremamente complessi** e computazionalmente difficili per poter aggiungere blocchi alla blockchain. Tale funzione produce un tipo di dati molto specifici che vengono utilizzati per verificare che sia stata eseguita una notevole quantità di lavoro.

Un **sistema POW** è una misura economica per scoraggiare attacchi e altri abusi di servizio, imponendo alcuni lavori che richiedono elevato tempo di elaborazione di un computer. Una caratteristica chiave di questi lavori è la loro asimmetria: il lavoro deve essere moderatamente, ma facile da controllare.

Teoria dei giochi: i nodi del network concorrono tra loro per registrare il nuovo blocco ottenendo di conseguenza un compenso. Grazie al compenso atteso la maggior parte dei nodi hanno interesse a comportarsi in maniera "legittima" contribuendo così alla crescita della blockchain.

Non solo PoW…

La Proof of Stake costituisce un metodo alternativo, un modo attraverso cui i nodi raggiungono un consenso.

Nel modello di consenso Proof of Srake, il numero di token di valuta digitale detenuti da ciascun utente, è una questione importante all'interno del sistema. Più grande è la partecipazione ("*stake*"), ovvero la quantità di token posseduti da un utente, maggiori sono le probabilità che non si stia violando il sistema. Ancora, più un individuo è esposto ad una criptovaluta, più è probabile che questi si comporti in modo ottimale.

I blocchi della Proof of Stake, a differenza dei blocchi della Proof of Work, non vengono estratti, ma coniati. I partecipanti che possiedono una partecipazione significativa nei sistemi Proof of Stake vengono selezionati su base pseudocasuale per coniare i blocchi e aggiungerli alla blockchain.

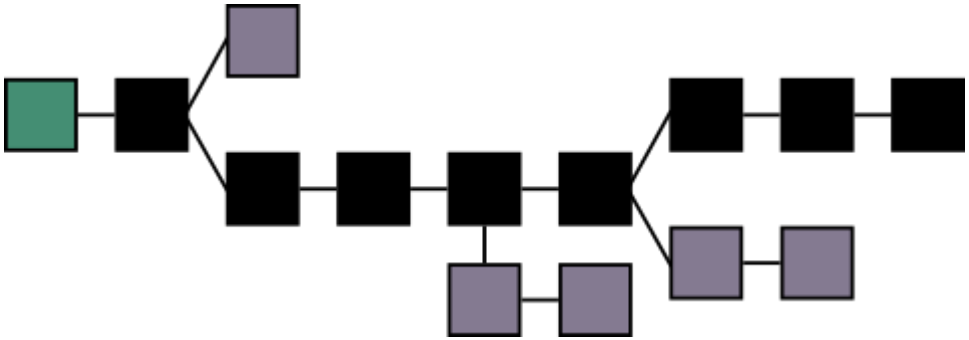
Ricapitolando…

La Blockchain è un **registro pubblico delle transazioni Bitcoin** in ordine cronologico. È utilizzata per memorizzare in modo permanente le transazioni Bitcoin e per prevenire double spending.

Come suggerisce il nome, la Blockchain è un insieme di blocchi fra loro concatenati: ogni blocco è identificato da un codice, contiene le informazioni di una serie di transazione, e contiene il codice del blocco precedente, così che sia possibile ripercorrere la catena all'indietro, fino al blocco originale. Un DNA delle transazioni Bitcoin.

Tutti i nodi della rete memorizzano tutti i blocchi e quindi tutta la Blockchain

La catena è unica



La catena è unica: se si vengono a creare due catene diverse (ad esempio, per un ritardo dell'aggiornamento dei blocchi), automaticamente quella ‘‘errata’’ viene cancellata e sovrascritta da quella corretta.

Per determinare la catena corretta, ci sono automatismi: la catena ritenuta corretta è sempre quella più lunga (*longest chain rule*).

Generalmente la catena più lunga è anche quella memorizzata dalla maggioranza dei nodi della rete (50%+1 rule), dato che i miner sono costantemente incentivati a creare blocchi validi (ovvero fare i bravi) attraverso le fee e i bitcoin generati ad ogni risoluzione del problema di mining.

Da un punto di vista della teoria dei giochi, collaborare alla catena più lunga è un equilibrio, dato che nessuno può ottenere un risultato migliore per se stesso (senza collaborare con altri) creando blocchi non validi (PoW).

Ciò rende molto difficile per un hacker modificare anche solo l'ultimo blocco.

Keywords 3: Generazione di nuova moneta

Si è parlato di costo computazionale, ma chi remunera i nodi?

Il sistema stesso: è presente un algoritmo di generazione di nuovi Bitcoin, e la valuta digitale generata viene data ai nodi. Inoltre vi sono delle fee per ogni transazione progettata.

Questo è un passaggio chiave!!!

I bitcoin generati e dati ai miner come ricompensa sono stabiliti a priori e non dipendono dalla potenza di calcolo della rete (dimezzano ogni tot) e ad un certo punto l'unica ricompensa che i miner riceveranno saranno le fee.

Ciò che dipende dalla potenza di calcolo è la complessità del problema di mining. Questa complessità viene regolata in modo tale che ci vogliano mediamente 10 minuti affinché la rete, nel suo complesso, crei un nuovo blocco.

In media, nota la potenza di calcolo della rete e la propria potenza di calcolo, ogni miner può calcolare ogni quanto riuscirà a minare un blocco, e capire così se per lui il mining è un gioco profittevole (considerando costi di energia e valore del bitcoin in quel periodo).

Quanto costa produrre un Bitcoin?

Se fino a qualche anno fa un buon computer era sufficiente per produrre (*minare*) Bitcoin, oggi sono necessari migliaia di processori e schede grafiche potentissime.

Per l'estrazione dei bitcoin sono stati messi a punto computer con processori specifici chiamati ASIC (*application-specific integrated circuits*); questi processori, oltre ad avere un costo elevato, comportano anche un alto consumo di energia elettrica.

Secondo alcuni studi effettuati, l'energia richiesta dai pc per validare una singola transazione può arrivare fino a 215 Kwh. Se si tiene conto che in tutto il mondo vengono completate circa 350 mila transazioni di Bitcoin al giorno, il consumo di energia è paragonabile a quello di alcune nazioni come Irlanda, Danimarca o Serbia.

Minare bitcoin significa quindi impiegare cifre considerevoli in energia elettrica e componenti hardware.

Ricapitolando

- Sicurezza: database distribuito all-over-the world + crittografia (tutto merito della tecnologia Blockchain)
- Senza intermediario (*trust*): consenso automatico (merito della tecnologia e di Bitcoin → *Currency On The Ledger*)
- Remunerazione dei nodi automatica: generazione di nuovi Bitcoin

Non solo Bitcoin… Ethereum

Gli Smart Contract

Ethereum

- E’ un’altra piattaforma basata su tecnologia blockchain
- Per poter girare sulla rete peer-to-peer gli address di Ethereum pagano l'utilizzo della sua potenza computazionale tramite una unità di conto, detta **Ether**, che funge quindi sia da criptovaluta che da carburante.
- Ethereum è diverso dalla blockchain di Bitcoin in quanto consente di creare Smart Contracts. Anche in Bitcoin si possono creare degli smart contract elementari. In Ethereum la particolarità è che sono basati su un linguaggio Turing completo

Smart Contract: «code-is-law»

Uno Smart Contract è la *trasposizione* in *codice* di un contratto in modo da verificare in automatico l'avverarsi di determinate condizioni (*controllo di dati di base del contratto*) e di *autoeseguire* in automatico azioni (*o dare disposizione affinché si possano eseguire determinate azioni*) nel momento in cui le condizioni determinate tra le parti sono raggiunte e verificate.

In altre parole lo Smart Contract è basato su un codice che "*legge*" sia le clausole che sono state concordate sia la condizioni operative nelle quali devono verificarsi le condizioni concordate e si autoesegue automaticamente nel momento in cui i dati riferiti alle situazioni reali corrispondono ai dati riferiti alle condizioni e alle clausole concordate.

Uno smart contract può contenere informazioni e regole (ad esempio, se A invoca f con input x, allora scrivi y).

- Uno smart contract è un programma che gira sulla macchina virtuale decentralizzata di Ethereum.
- Lo smart contract non può agire in modo attivo (ad esempio, non può monitorare lo stato di un altro smart contract e agire di conseguenza), ma agisce in modo reattivo (un utente, non necessariamente direttamente, deve invocarlo affinché compia qualunque operazione).

- Lo smart contract non può interrogare il mondo esterno alla blockchain. Ad esempio, in caso di una scommessa sportiva gestita attraverso uno smart contract, questo non può ottenere da un sito web il risultato della partita e agire di conseguenza.
- Lo smart contract può invece ottenere informazioni servendosi di oracoli.
- Gli oracoli sono smart contract in cui informazioni provenienti dal mondo esterno sono caricate in cambio di una reward.

Attivazione di uno smart contract: oracolo

AXA goes blockchain with fizzy

AXA is the first major insurance group to offer insurance using blockchain technology. Discover fizzy, a 100% automated, 100% secure platform for parametric insurance against delayed flights.

ALL NEWS | DIGITAL
SEP 13, 2017

fizzy is a fresh new genre in insurance. It offers direct, automatic compensation to policyholders whose flights are delayed. If your plane is more than two hours late, fizzy will reimburse you immediately.

Jun 15, 2016 | William Suberg | 5907

EU's Biggest Insurer Allianz Successfully Tests Smart Contracts

Europe's biggest insurer Allianz has stated it has successfully tested the use of smart contracts to improve natural disaster bond settlements.

Smart Contract e applicazioni finanziarie

Sistema decentralizzato -> Smart Contract, ovvero Code-is-law

Transazioni automatizzate: immaginando una piattaforma comune per le transazioni, due controparti definiscono il codice che regola gli scambi di denaro. Il codice è in tutto e per tutto il contratto

DLT+Smart Contract: Potrebbero essere potenzialmente utilizzati ad esempio per il posting di collaterale, rendendo le procedure più efficaci e veloci

Posting di un collateral

In alcuni casi viene richiesto alle controparti di un contratto finanziario di postare un collateral come garanzia del pagamento di un debito. Questo permette di mitigare il cosiddetto rischio di controparte, dato che tale garanzia permetterà di rientrare del debito anche in caso di fallimento della controparte

Come potrebbe una DLT ottimizzare questa procedura?

1. Smart Contract
2. Cambio di consenso per una procedura più veloce (real time)

Cambio di consenso

- "consensus by reconciliation": processo che i mercati finanziari hanno eletto come loro sistema «checks and balances».
- Si tratta quindi di passare ad una nuova forma di "decentralized consensus": un meccanismo automatico che permetta di validare velocemente le transazioni.

Meccanismi per correggere transazioni errate?

Giurisdizione in caso di contrasti?

Smart Contracts

Automation is an incremental innovation driver which can reduce the likelihood of human errors. But taken to extreme disruptive limits, as it might happen in the so-called code-is-law smart-contract approach, it can trigger new error classes of potentially humongous consequences. The reader is referred to the Ethereum TheDAO incident: an unknown attacker drained about $60m worth of the digital currency ether from TheDAO's $150m pool, just exploiting a flaw (undocumented feature?) in TheDAO's smart contract. Subsequent attempts to fix the incident failed and required the last-resort measure of rewriting the blockchain transaction history; the betrayal of blockchain immutability and code-is-law paradigm resulted in network-wide controversies and overall confusion: in the end, ether has forked in two independent distinct instances. Since even this sub-optimal solution would be unfeasible for registered assets, the operational risks of smart-contracts should not be underestimated.

[ESMA Response]

Errori negli Smart Contracts: come li affrontiamo???

The DAO Accident

TheDAO, acronimo di "*Decentralized Autonomous Organization*", ovvero "*organizzazione autonoma decentralizzata*", era un fondo di investimento automatizzato, integralmente gestito da computer e basato sulla tecnologia blockchain: aveva raccolto oltre 150 milioni di dollari nel breve periodo in cui era stato aperto alla sottoscrizione del pubblico.

Un individuo o un gruppo di individui ha trovato una falla nello *smart-contract* per sottrarre fondi dalla "cassa" della TheDAO

- Il 28 maggio 2016 è stata lanciata la piattaforma software.
- Venerdì 17 giugno è stata oggetto di una sottrazione di fondi grazie ad una linea di codice “pensata male” che ha permesso di sottrarre fondi appartenenti a TheDAO stessa.

Se code-is-law, questa sottrazione è illegale?

Se la blockchain è immutabile, come si può cancellare?

Fork

Una **Soft Fork** è una operazione che aggiorna le funzionalità di Ethereum mantenendo però la retrocompatibilità.

Una **Hard Fork**, invece, è un aggiornamento del protocollo che rende obsolete le vecchie versioni di Ethereum.

"By 4pm local time, the consensus was that should a soft fork be deployed within 27 days, the attacker would not be able to retrieve the funds he had stashed into a child DAO.

A subsequent hard fork could even return all ether, including the DAO's 'extraBalance' and the stolen funds, back into a smart contract. That smart contract would contain a single function: withdraw().

This would make it possible for everyone who participated in the DAO to withdraw their funds: thanks to the support of the miners, and because nothing had been spent so far, nothing would be lost."

Cos'è successo?

E' stato fatto un hard fork, la blockchain è stata riscritta eliminando la transazione.

Come? Con il *consenso distribuito*! Più del 50% degli utilizzatori di Ethereum ha accettato l'aggiornamento.

"The super majority of people (89%) voted for the Hard-Fork"

Il consenso distributo supera l'immutabilità della Blockchain

Hashing e Notarization

La blockchain è come un libro contabile con un ordine di transazione distribuito tra molte entità in cui è possibile solo aggiungere dati e di cui ciascuno conserva una copia identica. Ciascun registro presente nel libro contabile ha una marcatura temporale, è immutabile e verificabile singolarmente.

Un hash con l'intera struttura contenente le impronte digitali dei file è registrato nella blockchain. Tutte le parti che hanno accesso alla blockchain possono verificare singolarmente l'autenticità di tali file.

Keywords

- Marcatura temporale immutabile nella blockchain
- Ancorare alla blockchain
- Come? Hashing

COME FUNZIONA?

- Viene fatto l'hashing del documento. Questo significa che il contenuto del document è riassunto, o meglio rappresentato, da una stringa di 64 caratteri (256bit).
- La stringa di 64 caratteri è quindi messa in una transazione della blockchain di Bitcoin (o altra) utilizzando il campo OP_RETURN.
- Un piccolo pagamento in Bitcoin viene effettuato per processare la transazione e registrarla sulla blockchain (si può anche fare una transazione di 0 bitcoin, quindi pagando solo il costo della transazione – variabile ma intorno a 0,00001 bitcoin).

Costo minimo di una transazione (indicativo)

1 Bitcoin = 8000 Euro
0,00001 Bitcoin = 0,08 Euro
NB. 1 Satoshi=10^{-8} Bitcoin: è l'unità più piccola della criptovaluta Bitcoin

Ovviamente abbiamo preso Bitcoin come esempio, ma la Notarization può essere fatta anche su Ethereum, o altra Blockchain.

OP_RETURN è un campo «libero» presente in ogni transazione Bitcoin: libero, ma di dimensioni limitate.

Per questo è necessario ideare una metodologia per «comprimere» il documento di cui si vuole fare notarization in una stringa, tramite l'HASHING

HASH function: funzione che prende un input e ritorna come output una stringa di 64 caratteri. L'input può essere del testo, una foto, etc.

L'hashing è irreversibile dato che conoscendo l'hash, è matematicamente IMPOSSIBILE dedurne il testo originale.

A timestamping proof standard

OpenTimestamps aims to be a standard format for blockchain timestamping. The format is flexible enough to be vendor and blockchain independent.

Eternity Wall

Messages lasting forever

Proof of existence

The original service has been discontinued the 31 December 2017
You will be able to verify documents created from this page but you will not be able to create new proof.
For creating new proof, please refer to OpenTimestamps.
You can also send an email to do@ots.pub , you will get a reply with the .ots receipts of the email body and of any attachment.

Drag & Drop or select a document to check if it has been notarized in the blockchain.
3768 documents notarized so far.

Drop here a document

Or click to select one

Hash function

“A hash function takes an input of any length and creates an output of fixed length.

It takes an input string and created a string of letters and numbers

“a0680c04c4eb53884be77b4e10677f2b”

This is referred to as the message digest.

It is also known as the digital fingerprint.”

Esistono diversi tipi di hash function

MD5: 2795ba32c0a01fba1bd78d0ca3b41255

RipeMD128: e14407339a8b38d7a46372898694d17b

SHA-1: 7a40f85a28207a0f3c1c8b4ab6d92005e593ee6c

SHA-256:
adf728d034cbe8e0c08a9fea0720782aa890e49f331fea5c483fd4fe8a03835c

Impronta digitale, è così?

E’ possibile che due file diversi riportino lo stesso Hash?

L'hash proietta una sequenza di dati teoricamente infinita, in un hash finito e di solito molto più corto del file originale, quindi è possibile capitino i doppioni.

Possibile, ma improbabile! E, con le più avanzate tecniche di hash è difficile (se non impossibile) usare questa vulnerabilità (nota come *Collision*) per modificare documenti a fini illegali

E poi… c’è l’*avalanche effect* (effetto valanga) è una proprietà per cui una piccola variazione nell’input A, produce una notevole variazione negli hash.

Un esempio

Un contratto viene registrato sulla blockchain tramite notarization

Una persona vuole modificare una parte del contratto e poi dimostrare che quello modificato è il contratto originale.

Come potrebbe fare? Dovrebbe

a) Modificare il contratto secondo i suoi fini

MA IN MODO CHE

b) L'hash del nuovo contratto sia uguale al vecchio

Sembra particolarmente improbabile che riesca a soddisfare sia a) che b)!!!!

"The answer is that it is NOT infinitely unique but the secret sauce is that it would take something like all the computers since the beginning of time a billion years to find a collision. ie two different inputs resulting in the same hash output. And that is good enough."

Hashing… non solo notarization

L’hashing è fondamentale per la blockchain: la PoW di Bitcoin si basa su questa operazione!

Our target is to find a variation of it that SHA-256 hashes to a value beginning with '000'. We vary the string by adding an integer value to the end called a nonce and incrementing it each time. Finding a match for "Hello, world!" takes us 4251 tries (but happens to have zeroes in the first four digits):

```
"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
"Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
...
"Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
"Hello, world!4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
"Hello, world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
```

4251 hashes on a modern computer is not very much work (most computers can achieve at least 4 million hashes per second). Bitcoin automatically varies the difficulty (and thus the amount of work required to generate a block) to keep a roughly constant rate of block generation.

Ricapitolando

DLT e settore finanziario

Non è ancora possibile pensare una DLT che sostituisca in toto il sistema di transazioni finanziarie (troppo su larga scala). Ma sarebbe possibile per due controparti creare una DLT e usarla per le loro transazioni

La crittografia usata in Blockchain potrebbe certamente essere considerata per rendere più sicuri gli attuali database

Esempi su piccola scala di applicazioni della DLT sono in evoluzione

Non solo finanza: La Blockchain può essere usata come registro in cui inserire qualsiasi tipo di informazione e di conseguenza anche un contratto, un atto o un certificato, evitando l'intermediazione di terze parti, ma mantenendo la garanzia di pubblicità

Stato della tecnologia DLT

E’ una tecnologia recente

Attualmente implementata su scala medio-piccola

Blockchain può essere pubblica o privata

Non è possibile capire se e come potrà essere utilizzata su grande scala (costi hardware, velocità del sistema)

Blockchain: sicurezza data dall’uso massiccio della crittografia e decentralizzazione

Scalabilità

MARKET CAP OF $76.856 BILLION

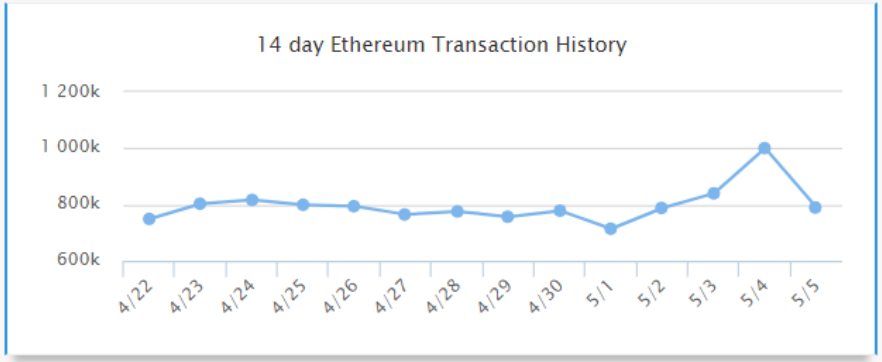
$774.23 @ 0.08137 BTC/ETH (-5.35%)

LAST BLOCK
5566910 (14.6s)

TRANSACTIONS
219.11 M (8.6 TPS)

Hash Rate
268,873.81 GH/s

Network Difficulty
3,242.03 TH



Blocks — View All

Block 5566910 > 49 secs ago	Mined By Ethermine	177 txns in 46 secs	Block Reward 3.2056 Ether
Block 5566909 > 1 min ago	Mined By PandaPool	103 txns in 7 secs	Block Reward 3.25673 Ether
Block 5566908 > 1 min ago	Mined By Nanopool	89 txns in 14 secs	Block Reward 3.31177 Ether
Block 5566907 > 1 min ago	Mined By Nanopool	54 txns in 4 secs	Block Reward 3.03268 Ether

Transactions — View All

TX# 0XD1E6F07530463CB8D56A137...	From 0x3f65732b7f2013ef... To 0x3d22287fcf804f47...	Amount 50 Ether	> 49 secs ago
TX# 0XB7AF2FA64D6848E6E7C1165...	From 0x072e8711704654... To 0x8f7dbf90e712855...	Amount 0 Ether	> 49 secs ago
TX# 0XEE15C7BD5576C87A6AD219E...	From 0x76543bb37e6d01... To 0xcb97e65f07da24d...	Amount 0 Ether	> 49 secs ago
TX# 0XF1CB0BD3A3D45BFEEF1D0A...	From 0x23ccbe4901ed51... To 0xe86a486976c613...	Amount 0.05529 Ether	> 49 secs ago

Scalabilità

Bitcoin – 3 to 4 transactions per second – 1 blocco ogni 10 minuti circa

Ethereum – 20 transactions per second – 1 blocco ogni 15 secondi circa

PayPal – 193 transactions per second average

Visa – 1,667 transaction per second

https://altcointoday.com/bitcoin-ethereum-vs-visa-paypal-transactions-per-second/

Scalabilità e Fiducia

La PoW è onerosa: è lei la causa principale dei problemi di scalabilità (oltre a problemi di memoria: tutti i nodi dovrebbero memorizzare tutte le transazioni).

Soluzioni allo studio: *operazioni off chain, proof of stake, proof-of-work solo su alcuni blocchi aleatori, permissioned ledgers*

Le **permissioned ledgers** (o blockchain private) possono essere controllate, e dunque possono avere una proprietà. Nel momento in cui un nuovo dato o record viene aggiunto alla blockchain, il sistema di approvazione non è vincolato alla maggioranza dei partecipanti ma a un numero limitato di attori che sono definibili come *trusted*.

DLT e settori finanziari: perché?

Tre falsi miti?

- Sistema meno oneroso
- Più sicuro
- Più veloce

Sistema meno oneroso!

- Le transazioni di Bitcoin su Blockchain non costano nulla.
- Ma questo è possibile perché vengono creati nuovi Bitcoin per la remunerazione dei nodi della rete che lavorano per il buon funzionamento del sistema

E se la generazione di nuova moneta non fosse permessa/possibile?

The mirage of low operational costs derives from the false impression of free blockchain transactions: if one takes into account the seigniorage revenues invested, each transaction on the bitcoin blockchain has a cost of about 5-10USD

[ESMA Response]

Sistema più sicuro

1. Potenzialmente sì: più sicuro in termini di immutabilità (a meno di 51% attack), ma non di privacy.
2. Il sistema di remunerazione dei nodi spinge ad usare la propria potenza di calcolo per far funzionare il sistema, non per cercare di forzarlo
3. Il database è distribuito all-over-the-world

Cosa succederebbe se 2 e 3 venissero meno ad esempio perché alcuni grandi intermediari lo gestiscono in proprio per il clearing delle loro transazioni?

Sistema più veloce? No, consenso più veloce!

- Il sistema di transazioni finanziarie attuali è “lento” non per una questione tecnologica, ma per una questione di consenso
- “consensus by reconciliation”: processo che i mercati finanziari hanno eletto come loro sistema «checks and balances».
- Si tratta quindi di passare ad una nuova forma di “decentralized consensus”: un meccanismo automatico che permette di validare velocemente le transazioni. Come in Bitcoin!

Meccanismi per correggere transazioni errate? In Bitcoin & Blockchain non sono presenti! Non possono essere presenti per come è disegnata la DLT!

La strada sembra promettente, ma… Problemi Aperti

- Cambio di consenso: è la strada che vogliamo percorrere?
- Smart Contract: sono sicuri? Come regolarli?
- Double Spending e reale disponibilità dell'oggetto transatto: *Currency on the ledger (bitcoin)* VS *Currency not on the ledger (fiat money).* Nel primo caso (Bitcoin) è possibile essere sicuri della reale disponibilità. Nel secondo?

Currency not on the Ledger

Come evitiamo il double spending?

Come possiamo essere sicuri della reale disponibilità dell'oggetto transatto?

➢Currency on the ledger (bitcoin), l'oggetto transatto è identificato univocamente dalla DLT

➢Sistema centralizzato (autorità tipo Banca centrale, clearing house)

➢Controllo esterno da terze parti

➢Fiducia???

Siamo davanti ad una tecnologia nata da poco, certamente innovativa

Non è ancora chiaro quali saranno i suoi usi e le sue potenzialità

Non è ancora chiaro come potrà essere implementata su larga scala

Ma…

E’ una tecnologia da seguire!!!