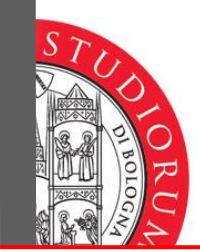
Modulo 1

Monica Palmirani

Tecnologie abilitanti la trasformazione digitale

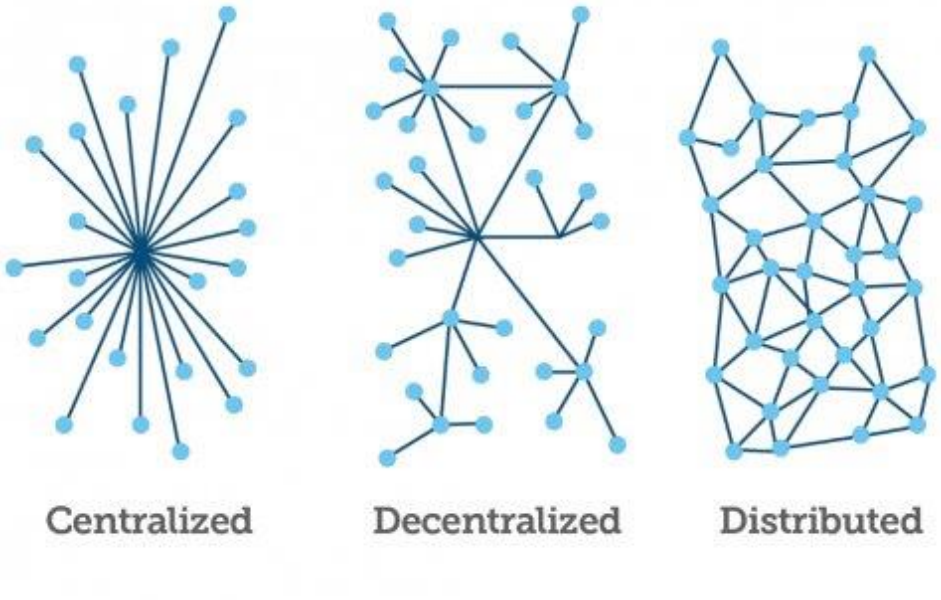
Part III



BLOCKCHAIN

Modelli di reti

- Centralized: un server
- Decentralized: molti server
- Distributed: peer-to-peer



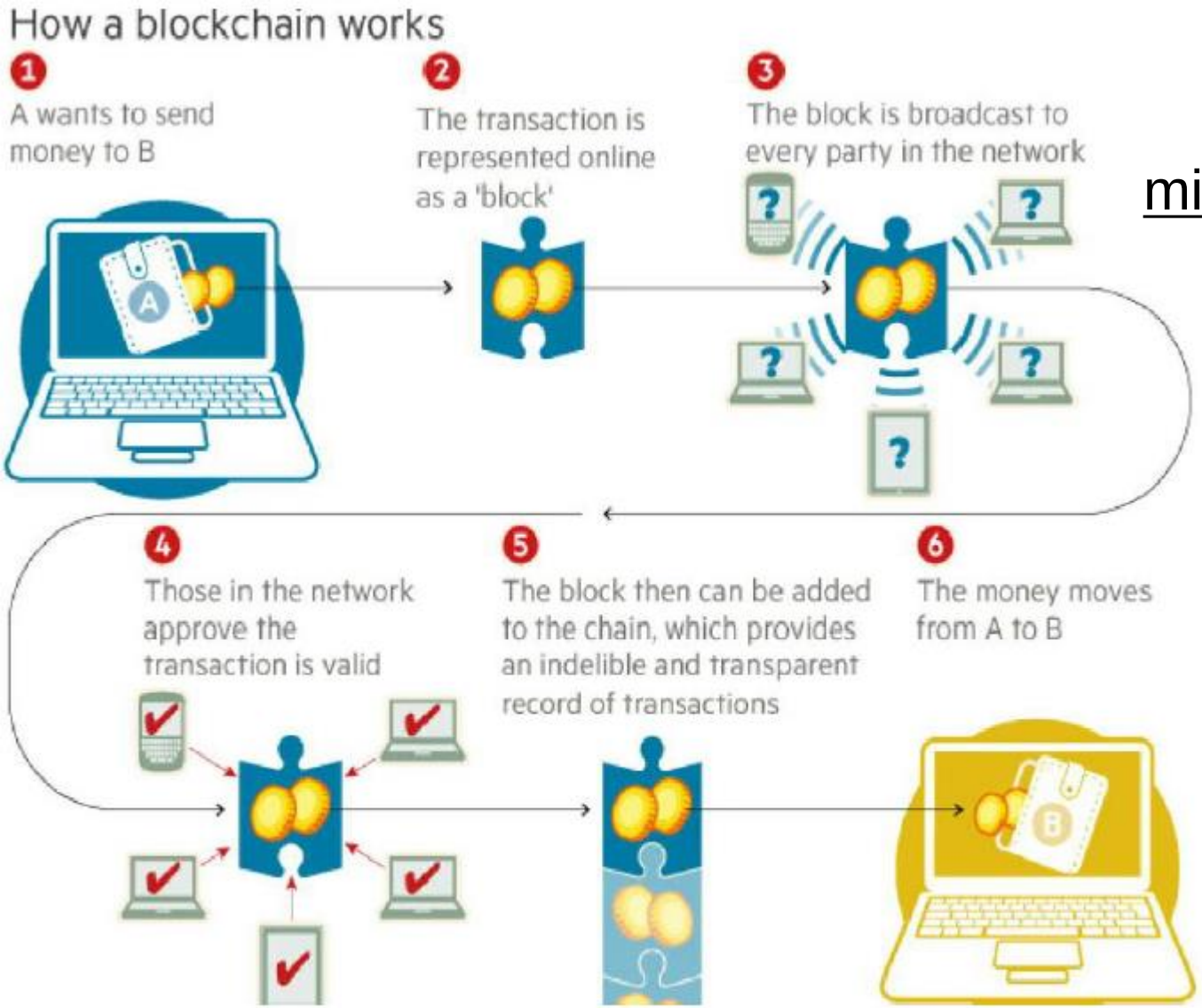
Tecnologie base

- firma digitale
- marca temporale (timestamp)
- merkle (hash) tree

Satoshi Nakamoto 2008

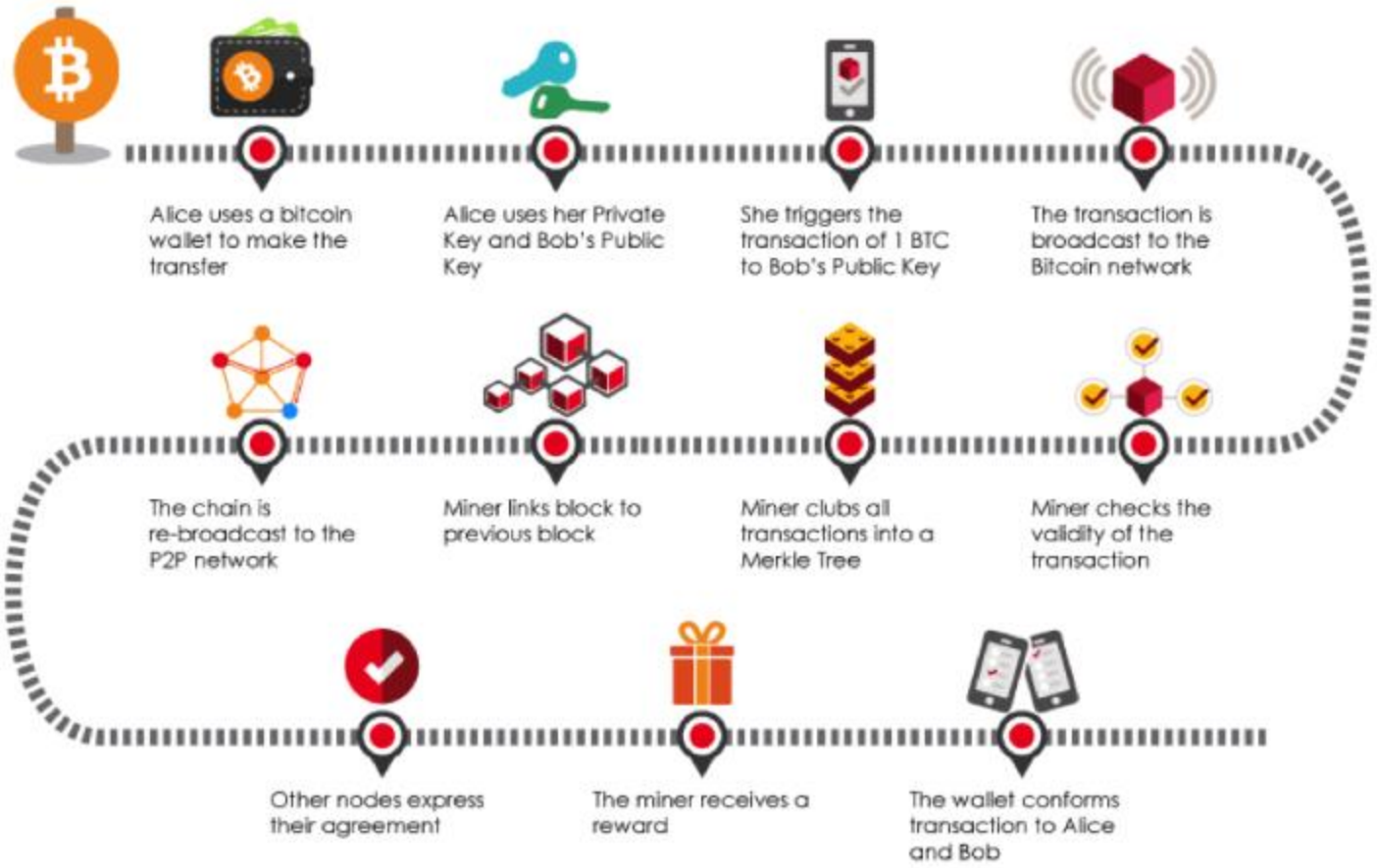
Come funziona il blockchain

- Ogni nodo/server tiene un registro (**ledger**) degli eventi di **blockchain**
- L'utente si rivolge ad una piattaforma per creare un **block** di un evento
- Ad ogni evento si crea un **block** che si unisce a quello precedente, il quale viene firmato e fissato con marca temporale
- Quando il block è completo viene inviato ai ***miner*** per la validazione
- Questo blocco entra nei registri distribuiti solo se risolto dal ***miner***
- Se il block viene scartato viene inserito nella **mempool**
- Si ottiene la ***validazione*** del blocco se è approvato dal 50%+1 dei registri (*miner*)
- **Consenso distribuito**



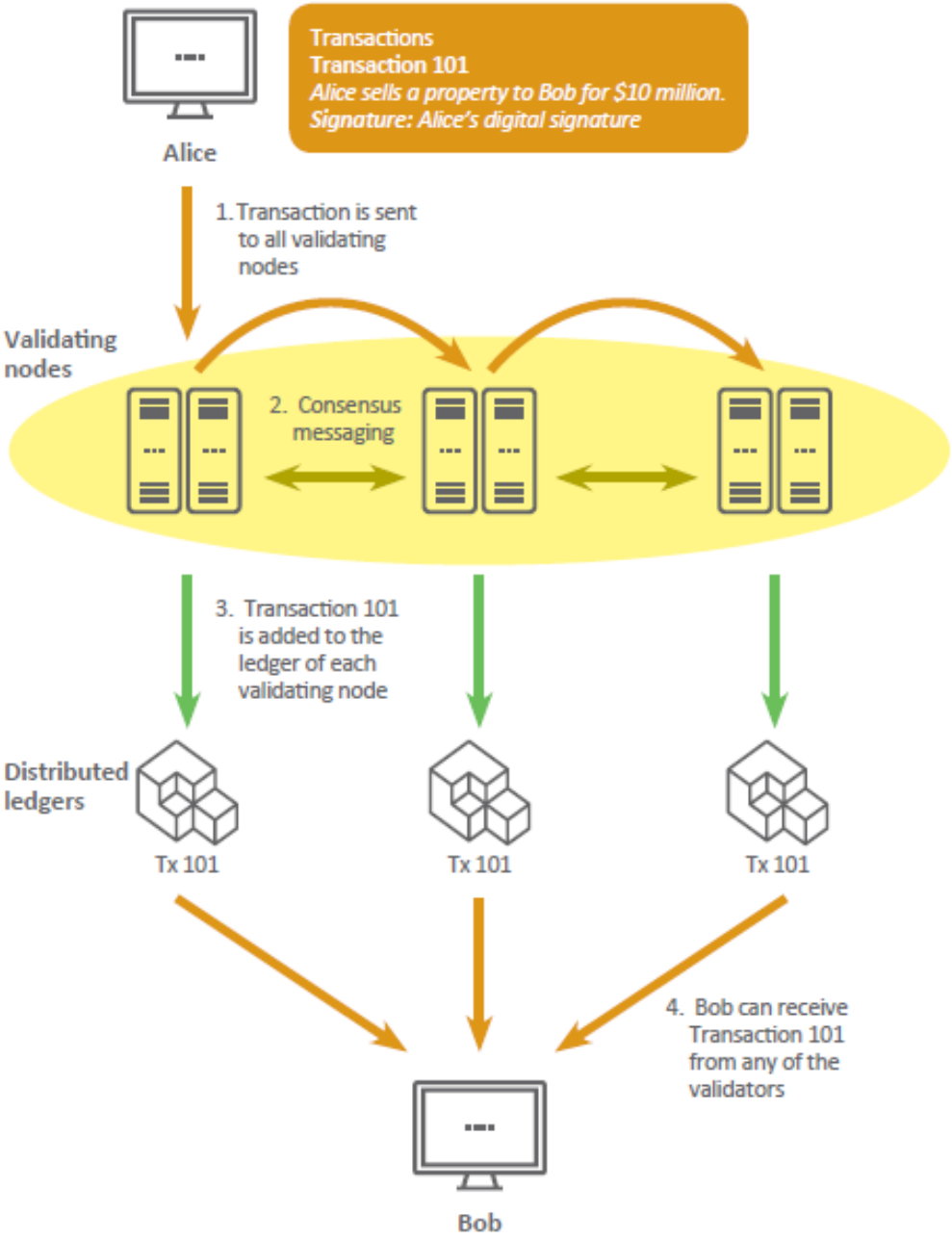
miners

Figure 2. Financial Transactions using the Blockchain technology[2].


Alice uses a bitcoin wallet to make the transfer
Alice uses her Private Key and Bob's Public Key
She triggers the transaction of 1 BTC to Bob's Public Key
The transaction is broadcast to the Bitcoin network
The chain is re-broadcast to the P2P network
Miner links block to previous block
Miner clubs all transactions into a Merkle Tree
Miner checks the validity of the transaction
Other nodes express their agreement
The miner receives a reward
The wallet conforms transaction to Alice and Bob

Whitepaper On
Distributed Ledger Technology

11 Nov 2016



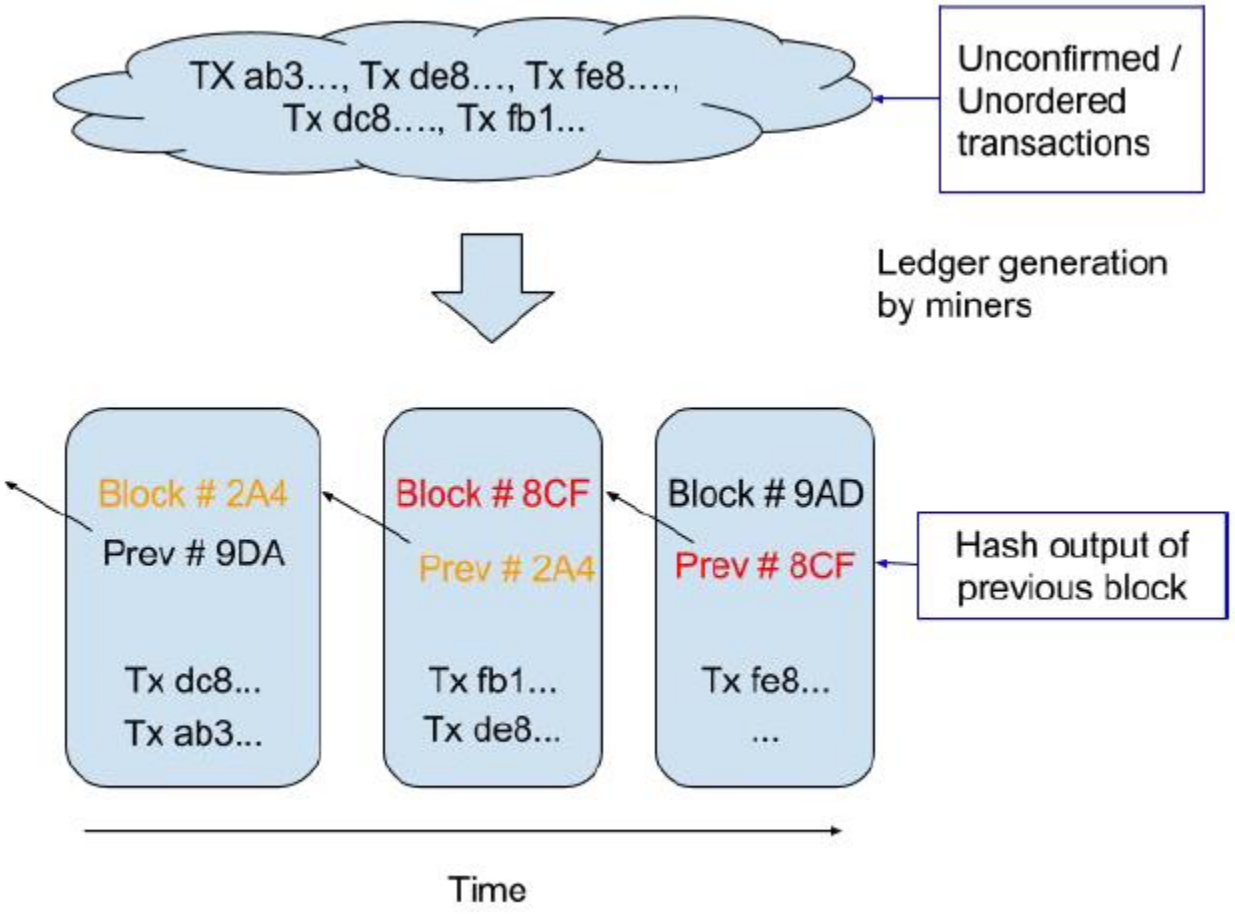
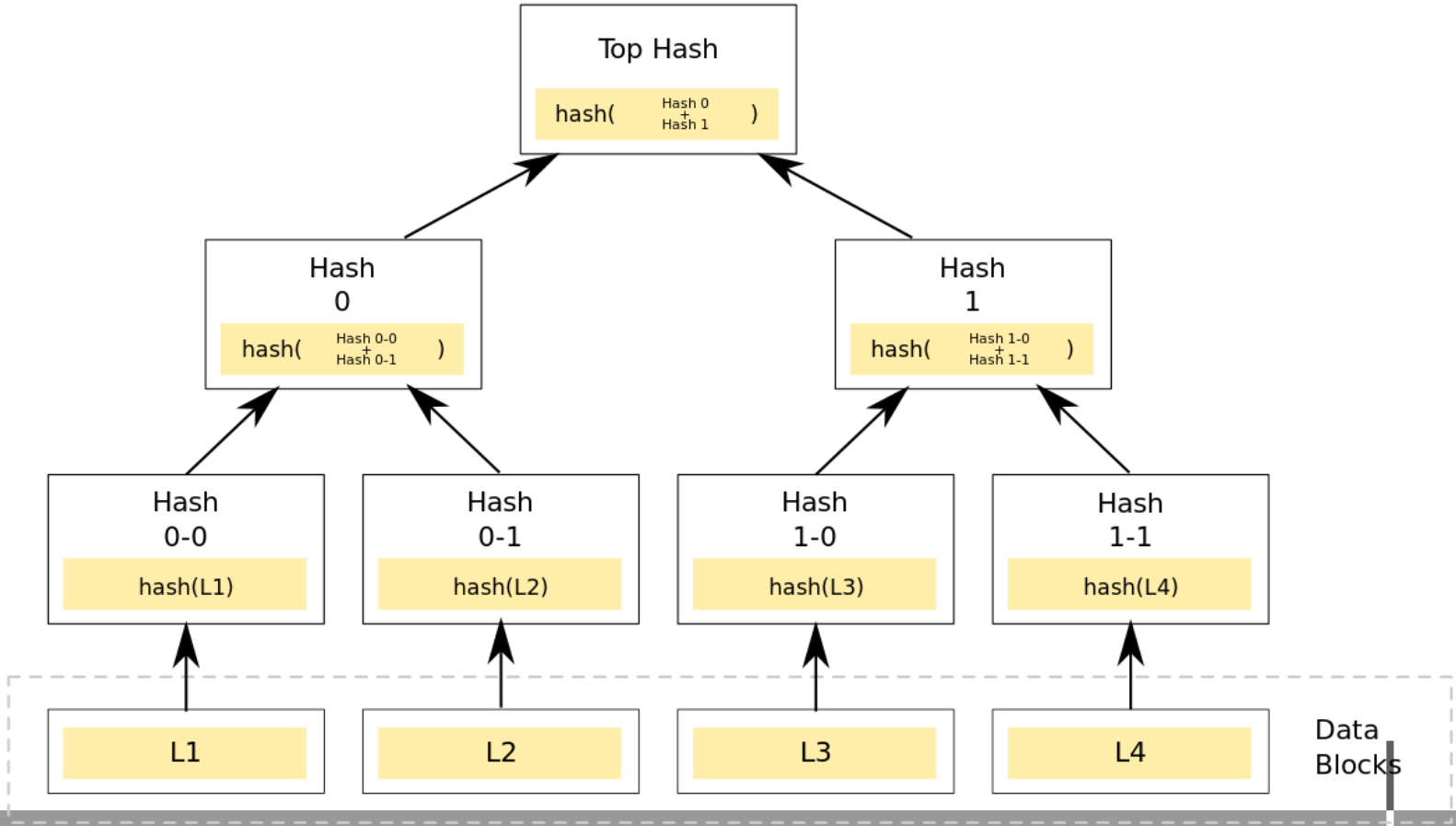
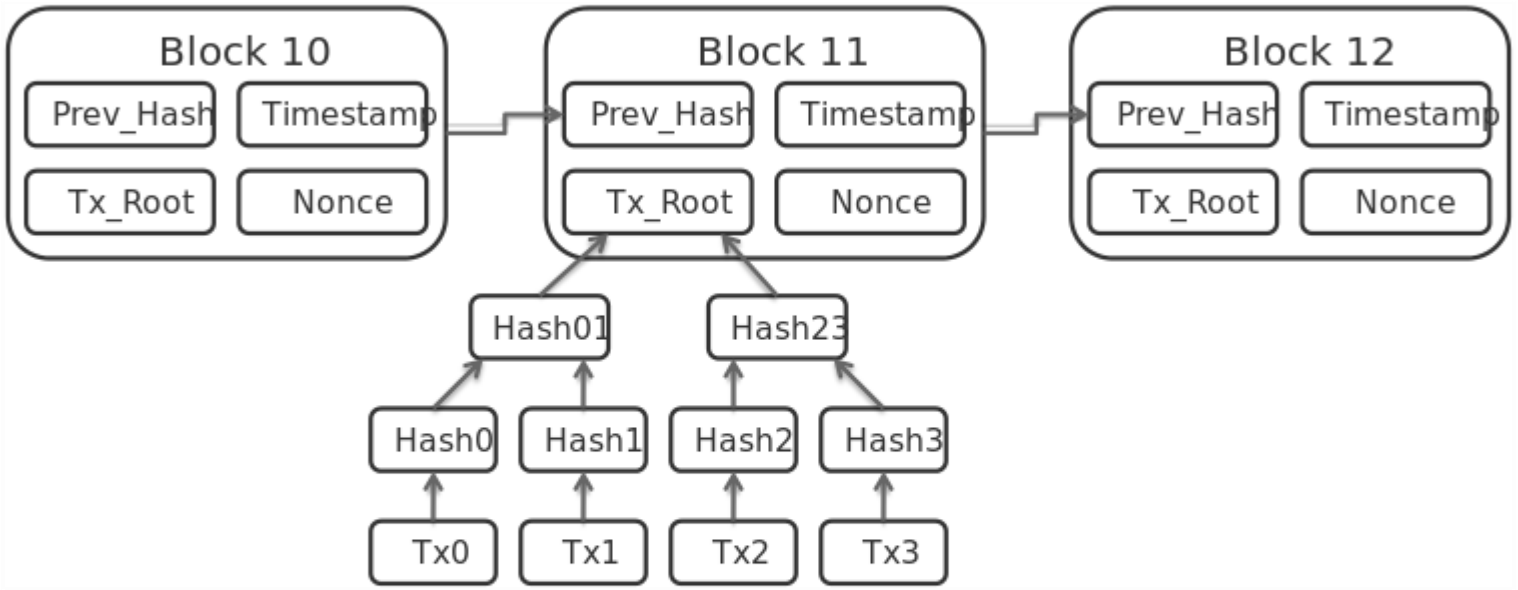


Figure 4. Generation of Blockchain from unordered transactions.

Merkle (hash) tree

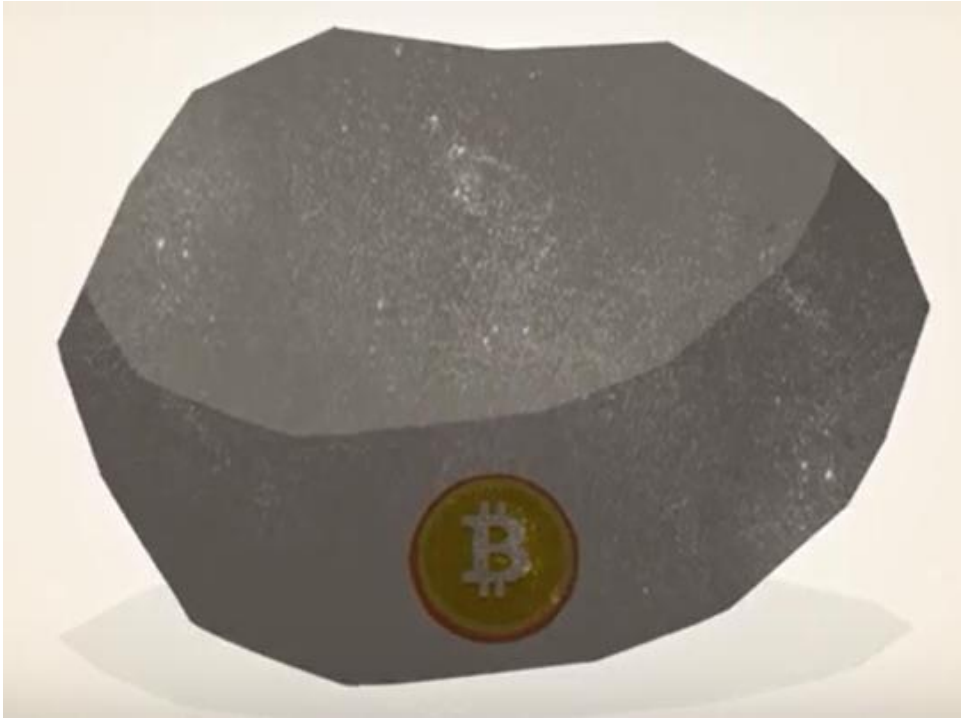
- http://onlinemd5.com/




Block 10
Prev_Hash
Timestamp
Tx_Root
Nonce
Block 11
Prev_Hash
Timestamp
Tx_Root
Nonce
Block 12
Prev_Hash
Timestamp
Tx_Root
Nonce
Hash01
Hash23
Hash0
Hash1
Hash2
Hash3
Tx0
Tx1
Tx2
Tx3

Verificare un blocco è costoso

- https://guadagnabitcoin.wordpress.com/bitcoin-mining/

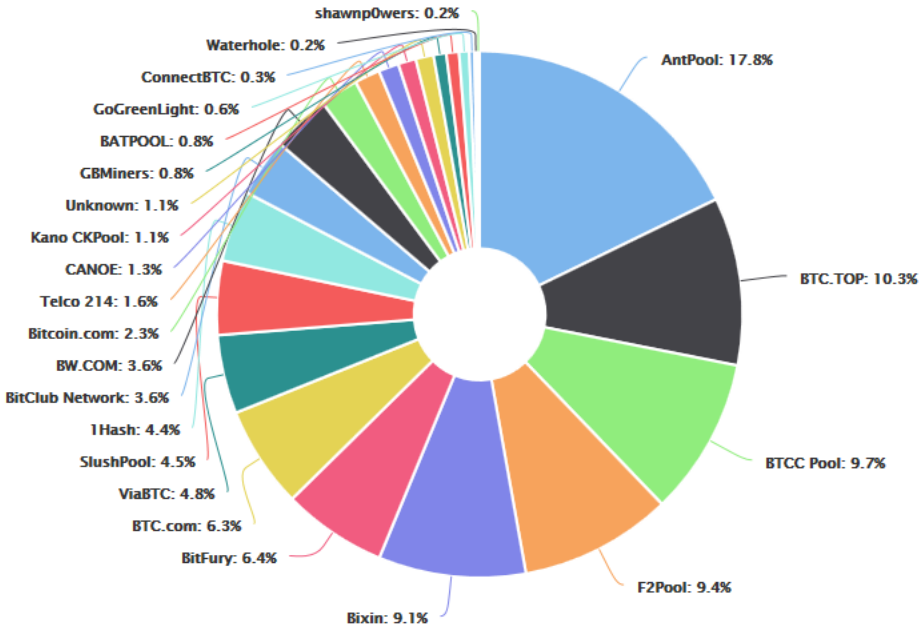


Minatori

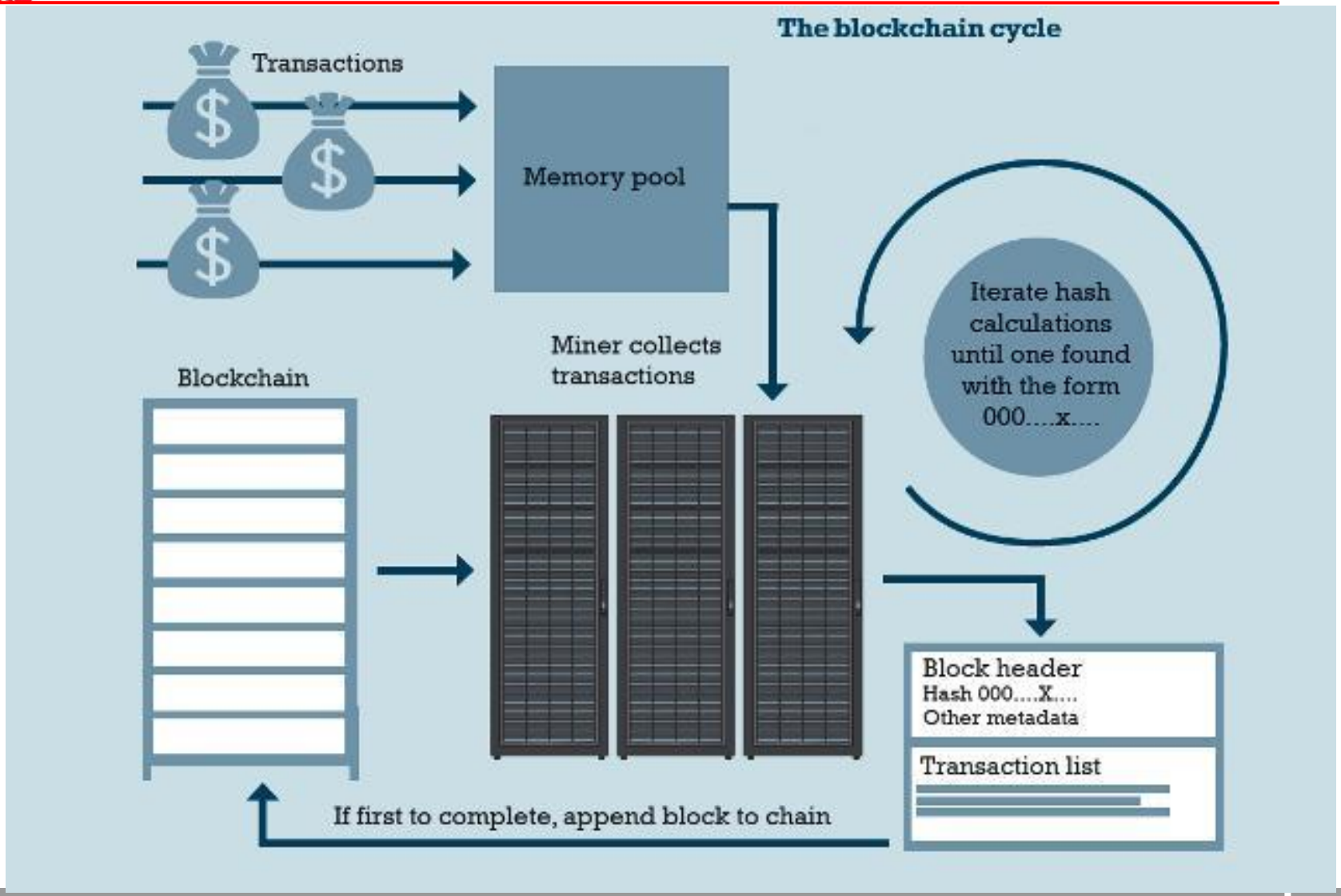
Distribuzione capacità di Hash Una stima della distribuzione della capacità di hash tra i principali gruppi di minatori

Il grafico qui sotto mostra la percentuale di mercato dei gruppi di minatori più popolari. Va considerato come una stima grezza e per vari motivi non sarà mai accurato al 100%. Una larga percentuale di blocchi Sconosciuti non significa che sia in corso un attacco alla rete, significa solamente che non siamo stati in grado di determinare la loro origine.

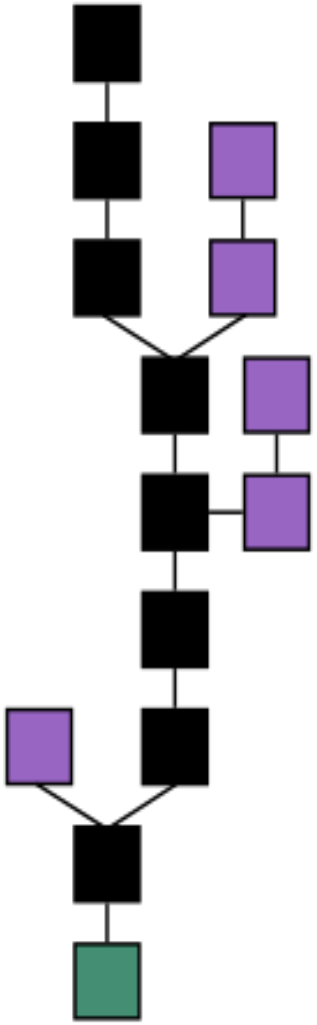
24 ore - 48 ore - 4 giorni

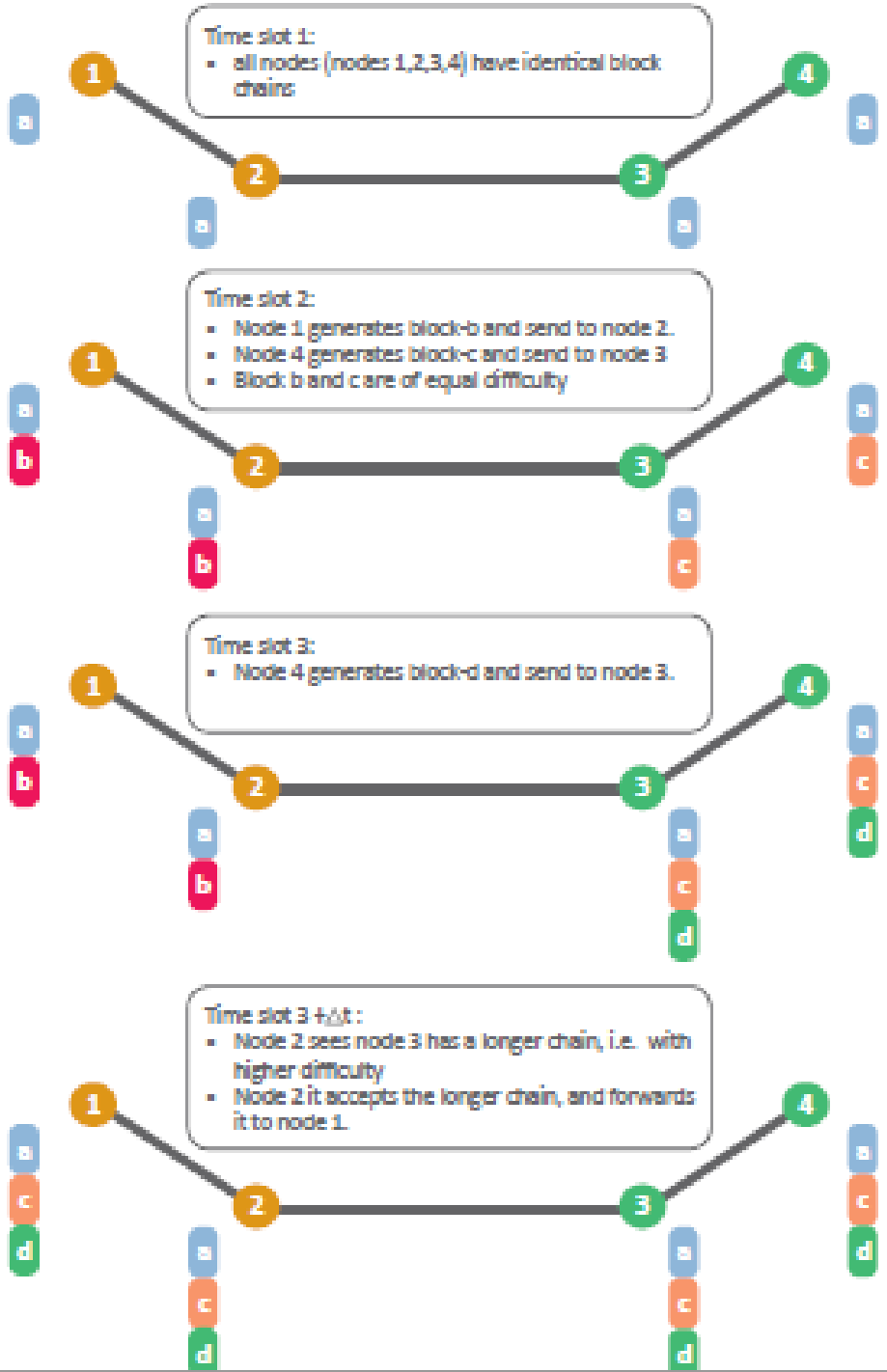


Mempool


The blockchain cycle
Transactions
Memory pool
Iterate hash calculations until one found with the form 000....x....
Miner collects transactions
Blockchain
Block header
Hash 000....X....
Other metadata
Transaction list
If first to complete, append block to chain

I blocchi orfani





Anatomia di un blocco

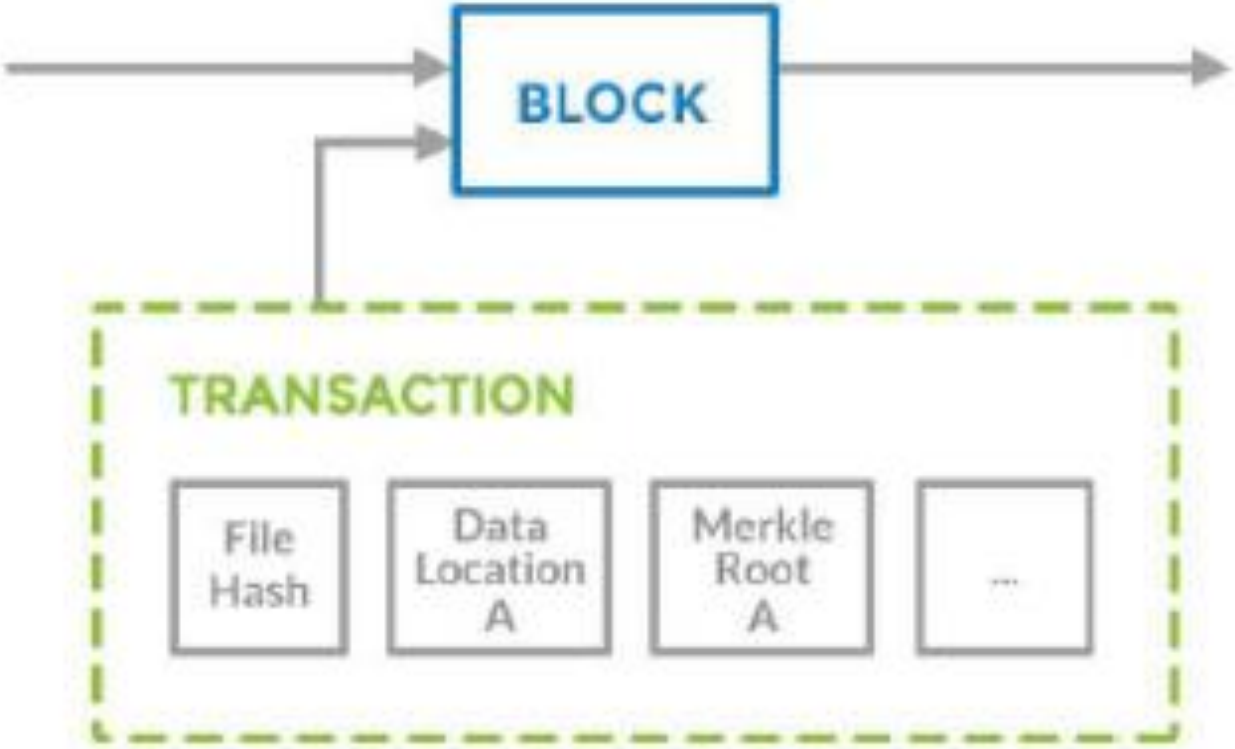
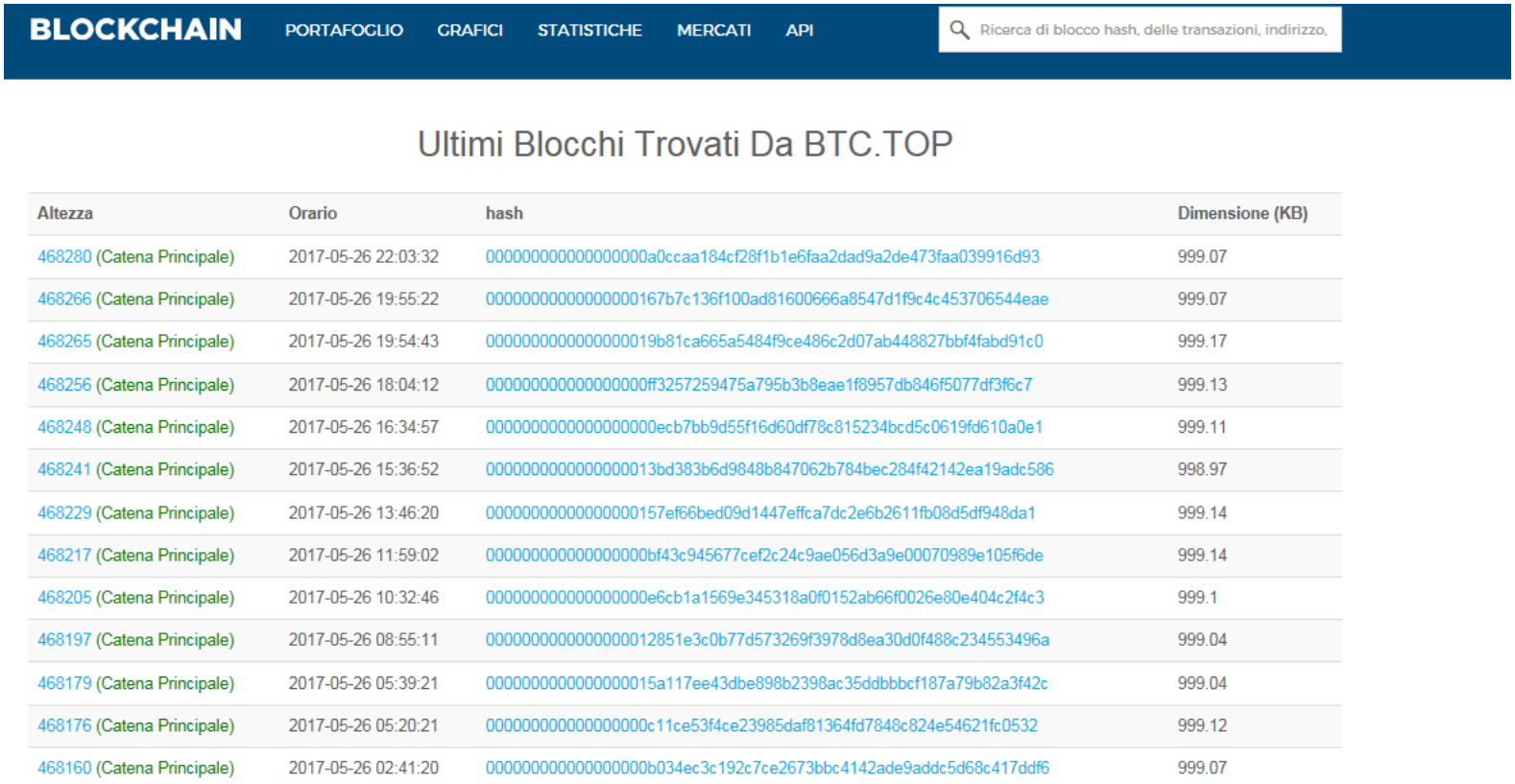
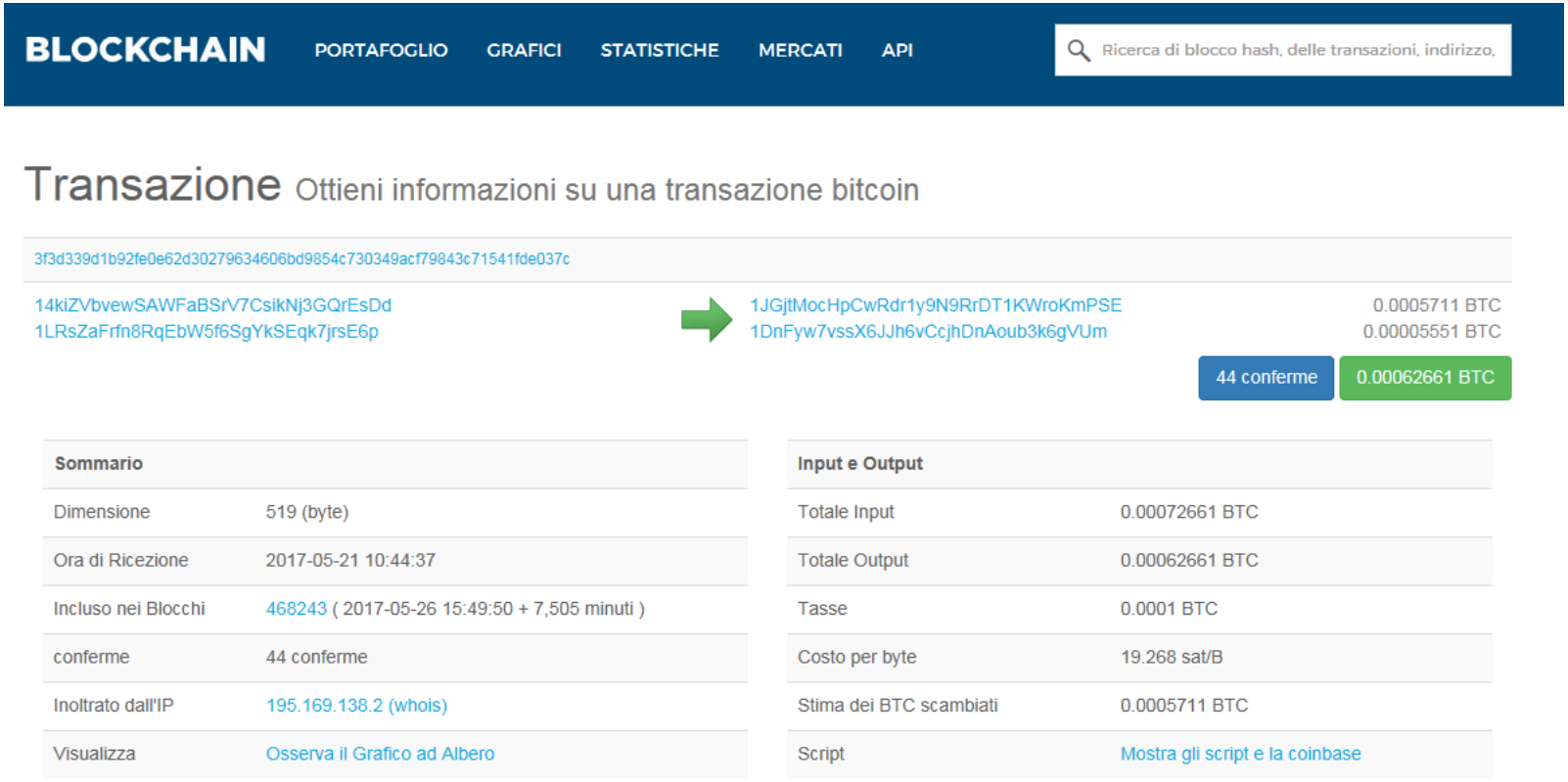


Figure 14 Metadata Insertion in the Blockchain[15].

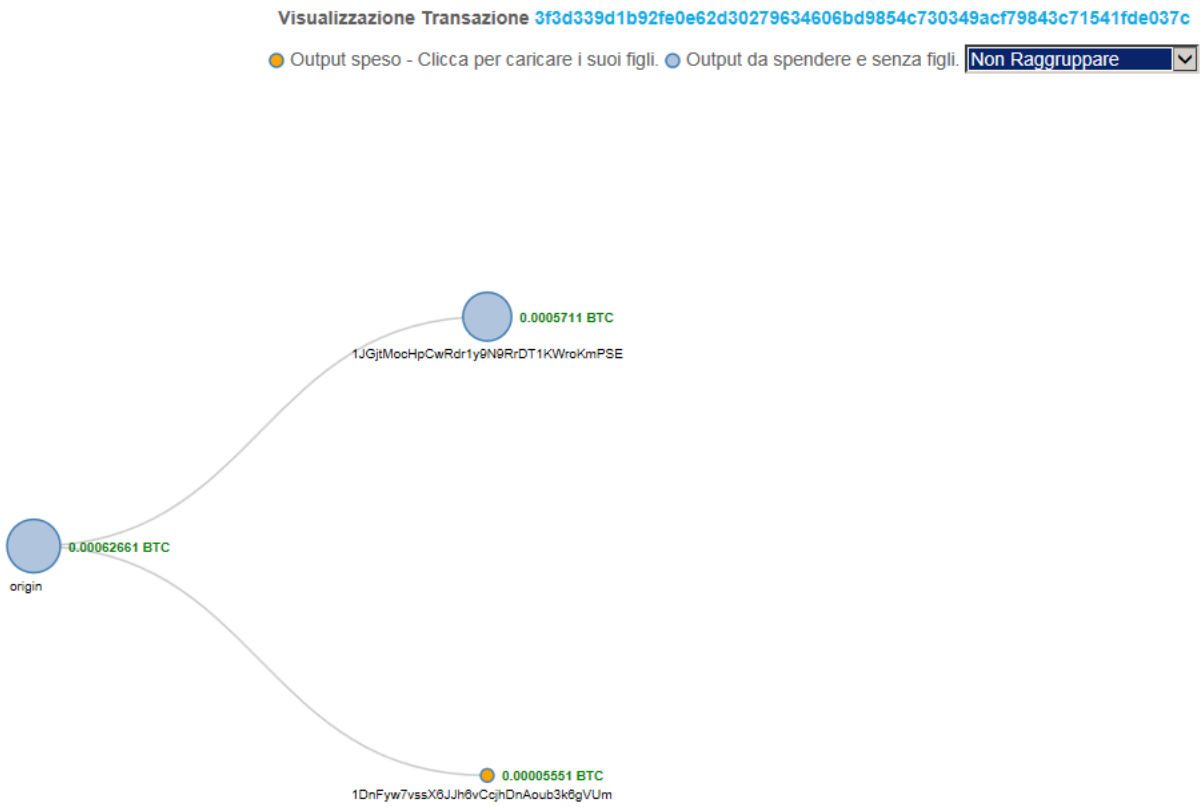
Esempio di registro

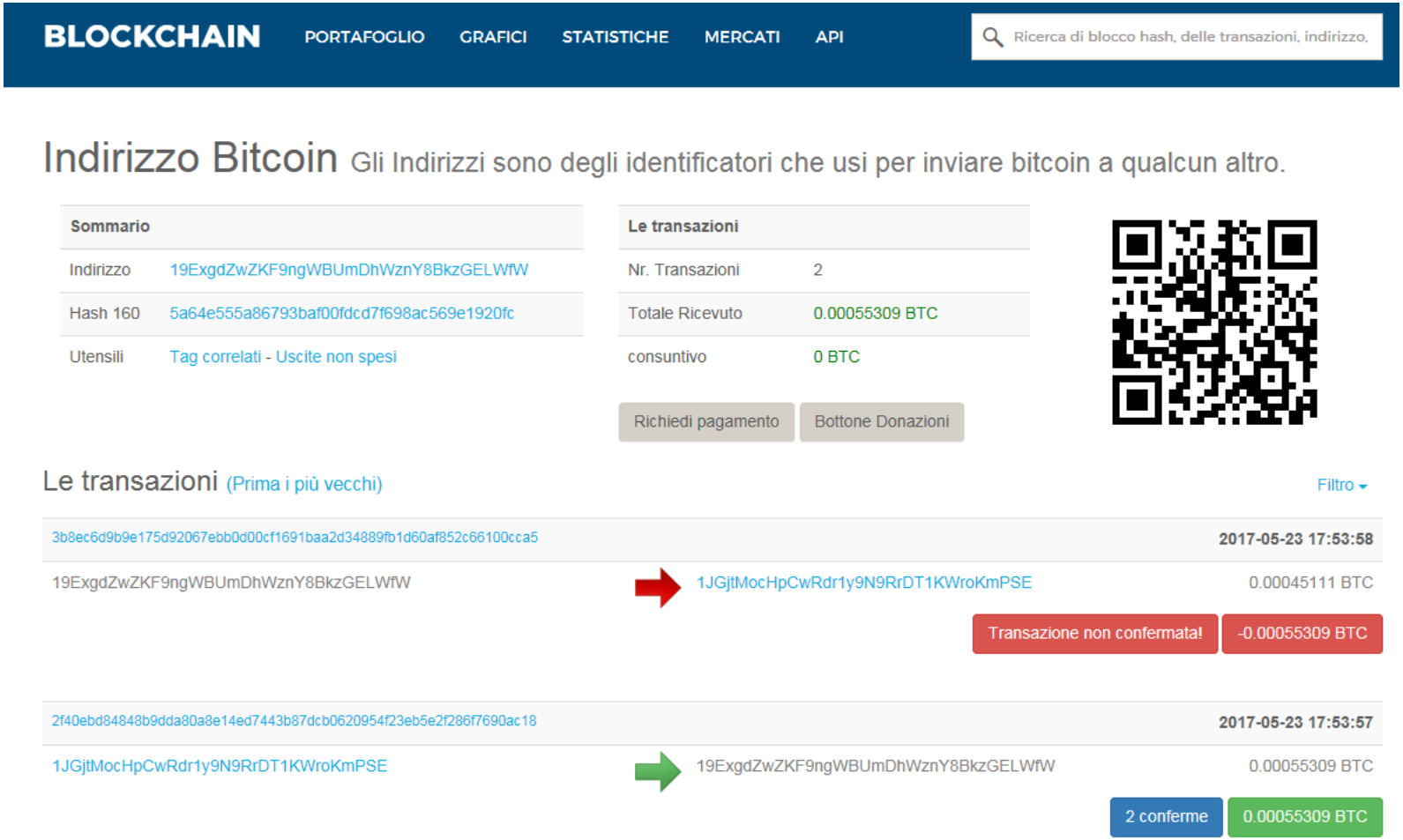


Anatomia di una transazione



Grafo di una transazione



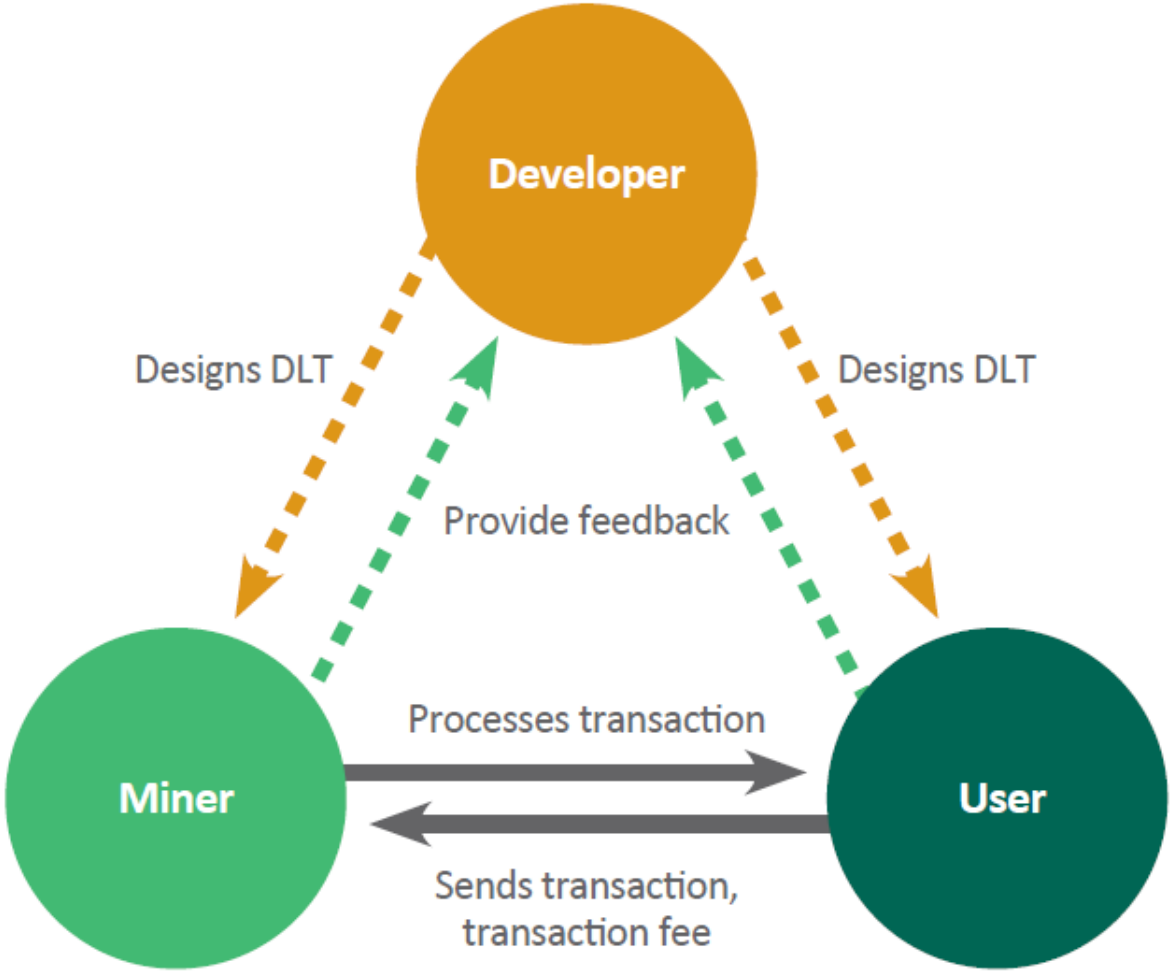

BLOCKCHAIN
PORTAFOGLIO
GRAFICI
STATISTICHE
MERCATI
API
Ricerca di blocco hash, delle transazioni, indirizzo,
Indirizzo Bitcoin Gli Indirizzi sono degli identificatori che usi per inviare bitcoin a qualcun altro.
Sommario
Indirizzo 19ExgdZwZKF9ngWBUmDhWznY8BkzGELWfW
Hash 160 5a64e555a86793baf00fdcd7f698ac569e1920fc
Utensili Tag correlati - Uscite non spesi
Le transazioni
Nr. Transazioni 2
Totale Ricevuto 0.00055309 BTC
consuntivo 0 BTC
Richiedi pagamento
Bottone Donazioni
Le transazioni (Prima i più vecchi)
Filtro
3b8ec6d9b9e175d92067ebb0d00cf1691baa2d34889fb1d60af852c66100cca5
2017-05-23 17:53:58
19ExgdZwZKF9ngWBUmDhWznY8BkzGELWfW
1JGjtMocHpCwRdr1y9N9RrDT1KWroKmPSE
0.00045111 BTC
Transazione non confermata!
-0.00055309 BTC
2f40ebd84848b9dda80a8e14ed7443b87dcb0620954f23eb5e2f286f7690ac18
2017-05-23 17:53:57
1JGjtMocHpCwRdr1y9N9RrDT1KWroKmPSE
19ExgdZwZKF9ngWBUmDhWznY8BkzGELWfW
0.00055309 BTC
2 conferme
0.00055309 BTC

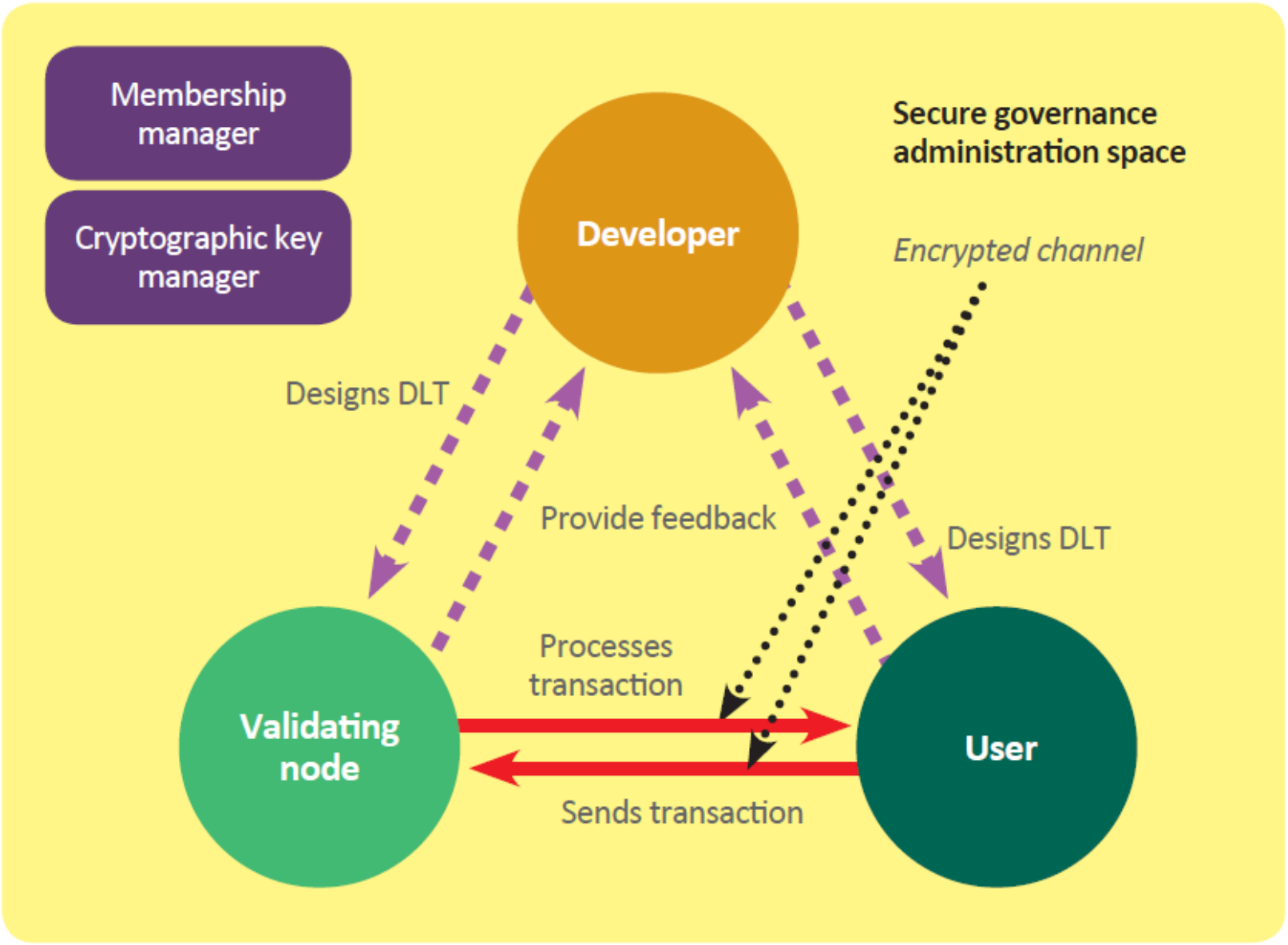

BLOCKCHAIN
PORTAFOGLIO
GRAFICI
STATISTICHE
MERCATI
API
Search for block hash, transaction, address, etc
Grafici sui Bitcoin
La fonte più attendibile per i dati sul blockchain bitcoin.
CURRENCY STATISTICS
BLOCK DETAILS
MINING INFORMATION
NETWORK ACTIVITY
WALLET ACTIVITY
STATISTICHE POPOLARI
Prezzo di mercato (USD)
$2,300.71
USD
Prezzo medio di mercato in USD nelle principali borse di cambio bitcoin.
Dimensione media del blocco
0.96
Megabytes
La 24 ore dimensione media del blocco in MB.
Transactions per Day
335,319
Transactions
Il numero complessivo di transazioni Bitcoin confermati nelle ultime 24 ore.
MemPool Size
111,775,207
Bytes
La dimensione aggregata delle transazioni in attesa di essere confermata.

Diversi modelli

- Pubblica: network pubblica
  - Tutti possono scrivere
  - Non servono permessi
  - Non c'è un punto di controllo
  - Anonima
- Privata: rete privata
  - Solo attori noti e identificati possono partecipare
  - La rete è gestita da un gestore
  - Non ci sono controllori
  - Non c'è anonimato

Attori coinvolti





A common governance structure of, and roles in, a permissioned DLT network

Unpermissioned vs. Permissioned

9.2 Privacy

Unpermissioned DLT Networks

User identities are pseudo-anonymous since only a limited amount of personal data and identity information is stored in unpermissioned DLT networks. Although transactions in an unpermissioned DLT network are usually unencrypted, they can only be traced to DLT wallet addresses, which are numerical strings associated with wallets but which do not reveal the wallet's private (secret) key, and do not expose much wallet owner information. This helps preserve privacy and hide the identity of the owner.

Users can further protect the privacy of their transaction history by utilising different DLT wallet addresses to conduct individual transactions.[17] This makes it very difficult for other parties to trace the owner's identity, or to identify the owners of the transactions and assets stored in the unpermissioned DLT network.

Permissioned DLT Networks

Transactions in a permissioned DLT network are encrypted to prevent unauthorised parties from reading them. Network communication among validating nodes and users is also encrypted to make data unintelligible even when intercepted during data transmission over the permissioned DLT network. Data privacy can be further protected by storing confidential data in a restricted location, with the DLT ledgers merely storing the hash of this data.

Anonimato vs. Legal control

The privacy challenge

In addition, there is always a challenge and in some cases a dilemma for an unpermissioned DLT network when faced with the need to protect user privacy while also being required to assist law enforcement authorities. Government authorities want to be able to detect illegal cryptocurrency activities such as money laundering, tax evasion, drug trafficking, and ransom payments. On the other hand, users may be concerned that details of their crypto-currency activities, and hence of their personal data and lifestyles, could be exposed to unauthorised parties. The challenge of dealing with the conflict between the need for users' privacy and the right for authorities to know about and monitor activities for various legitimate purposes cannot be underestimated.

Trasparenza vs. riservatezza

The privacy challenge

Sensitive transaction data in a permissioned DLT network often needs to be treated with confidentiality, and access to such data should be restricted to authorised parties only. Strong data encryption and adequate access controls are essential for protecting a permissioned DLT network. A permissioned DLT network should be carefully designed, with the security and data protection requirements being embedded at the system design stage and thoroughly scrutinised before implementation.

A node may serve the purpose of storing a ledger or a database. As new applications evolve for processing data in the DLT ledgers, the need will also arise for new cryptography technologies to ensure adequate data protection. For instance, a need may arise for carrying out a new kind of big data analysis on the records stored in a DLT ledger. To ensure the safety and efficiency of the DLT network, it would be desirable to be able to perform big data analysis on such records in an encrypted form. Also, advances in computing power (e.g. quantum computing) might one day render current encryption technology breakable. New cryptographic technology will always be needed over time to provide improved protection.

In addressing the challenge of balancing data privacy and data transparency so that authorities can carry out certain actions, permissioned DLT networks are obviously a better option. A permissioned DLT network can be designed in a way that meets data privacy requirements while at the same time complying with the requirements of law enforcement agencies and regulatory authorities. For example, since the members of a permissioned DLT are trusted and known parties, the accepted operating rules can specify the need for them to comply with local laws and regulatory requirements.

blockchain

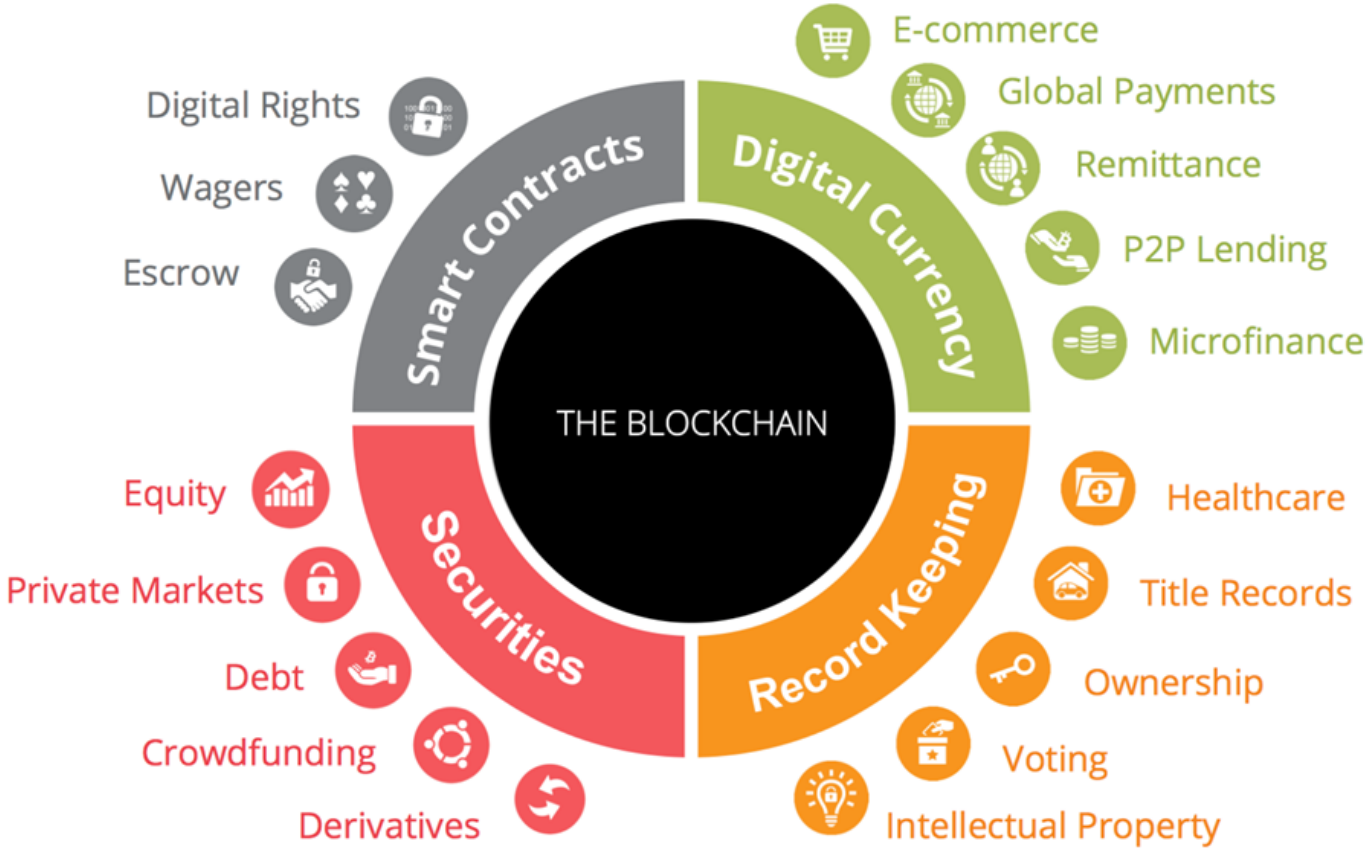
- Distribuito
- Sicuro
- Irrevocabile
- Accountable
- Trasparente
- Fra attori che non si conoscono
- In un processo

- Volume dei registri
- Costoso in termini di perfomance
- Conflitti di blocchi
- Blocchi orfani
- Privacy issues
- DDos e virus

IBM

Blockchain Potential Applications & Disruption

The blockchain is radically changing the future of transaction based industries



BLOCKTECH in FINANCIAL SERVICES VIRTUALscape

by William Mougayar

APPLICATIONS & SOLUTIONS

Brokerage
coinbase, BitPagos, Unocoin, BTCC, BITFINEX, CIRCLE, COINJAR, QUADRIGACX, bitFlyer, safello, volabit, coinfloor, coins.ph

Exchanges
BTer.com, coinbase, kraken, HUOBI.com, BITSTAMP, POLONIEX, BTC, bitcoin.de, GEMINI, mexbt, CAMP BX, BITSO, Coinffeine, PAYMIUM, CEX.IO, BitOasis, SHAPESHIFT, BTC express, coinsecure, coinsetter, Bits of Gold

Soft Wallets
BLOCKCHAIN, airBitz, coinbase, ARMORY, ELECTRUM, xapo, bread wallet, Coinkite, Mycelium, MultiBit HD, coinprism

Hard Wallets
TREZOR, case, Ledger Wallet, keep key

Microtransactions
BitMesh, BitWall, ChangeTip, ProTip, Strawpay

Investments
Grayscale, magnr, Loanbase, string, Yuanbao, KOIBANX, Bitbond, WeiFund, WEALTHCOIN, lighthouse, BSAVE.IO, dangpu.com, BTCjam, CHROMA.FUND

Merchants
bitpay, Bitnet, Coinkite, Coinify, PEY, CoinPayments, coinsnap, coinbase, CoinSimple, BITPagos

Compliance
ELLIPTIC, third key solutions, PROTUS, CHAINALYSIS, Sig3, BLOCKSEER, CryptoCorp, identityMind GLOBAL, Tradle, vogogo, COINALYTICS, BLOCKVERIFY, Merkle Tree

Trading Platforms
COINIGY, HEDGY, OrderBook, tradewave, COINUT, AltOptions, COINIGY, MAKER, BITNOMIAL, TERA EXCHANGE, BitMEX, Mirror, CRYEX, 1Broker, TABTRADER, DXmarkets, AlphaPoint, NOBLE MARKETS, HitFin

Capital Markets
Chain, symbiont, NASDAQ Private Market, Digital Asset Holdings, clearmatics, itBit, TradeBlock, t0, epiphyte

Money Services
CRYPTOPAY, cashila, ABRA, Fuzo, tether, BitwalaBitwala, coins.ph, Simplex, ATLAS, BITX, coinx, REBIT, uphold, SecureCoin, DUO MONEY, BITNEXO, CoinPip, LocalBitcoins.com, BitPesa, BlinkTrade, COINAPULT, MELOTIC, Glidera, bridge21

Financial Data
bitcoinity., CoinMarketCap, CryptoCoin, BRAVE NEW COIN, BlockJockey, CRYPTRADER, BitcoinWisdom, TradeBlock, CoinGecko, Coinhills

Payments
Align Commerce, GOCOIN, About Payments, BLADE, GAZEBO.IO, GemPay, cuber, SETL.io, safecash

ATMs
LocalBitcoins.com, Robocoin, bitxatm, bitaccess, Project Skyhook, btcpoint, SERY, LAMASSU BITCOIN VENTURES, GB, genesiscoin, COINOUTLET, Modenero Concierge

Trade Finance
GAZEBO.IO, everledger, CHRONICLED, WAVE, skuchain, digix, PROVENANCE, thingchain

Payroll & Insurance
paybits, bitWAGE, DYNAMIS

Banks
BBVA, UBS, LHV, London Stock Exchange, secco, BNY MELLON, BARCLAYS, fidor BANK, citibank, moni

MIDDLEWARE & SERVICES

Services
CRYPTONOMEX, B9, CONSENSYS, SolidX, appliedblockchain, RUBIX

Software Development
chainscript, HydraChain, Blockstack.io, PEERNOVA, openchain, CREDITS, eris INDUSTRIES, MultiChain, Manifold, Blockstream

General APIs
BitGo, neuroware, coinbase, bitcore, Gem, BLOCKCYPHER, Coinkite

Special APIs
TIERION, Open Assets, bitbind.io, COLOREDCOINS, colu, factom, ChromaWay

Platforms
Counterparty, Monetas, Omni, erocoin, blockstack, HYPERLEDGER, Tendermint, BLOCKAPPS, appliedblockchain

Smart Contracts
SmartContract, CoinSpark, ETH BaaS, ROOTSTOCK, bitShares, Tembusu Systems

INFRASTRUCTURE & BASE PROTOCOLS

Public
bitcoin, bitShares, ethereum

Special
ripple, stellar

Payment
Amiko Pay, MONERO, Lightning Network

Miners
ANTPOOL, BitFury, 21 INC, BTCC, BITCOINCZ

Source: http://startupmanagement.org/blog

Table of contents

European Parliament

How blockchain technology could change our lives

IN-DEPTH ANALYSIS

EPRS | European Parliamentary Research Service

Author: Philip Boucher

Scientific Foresight Unit (STOA)

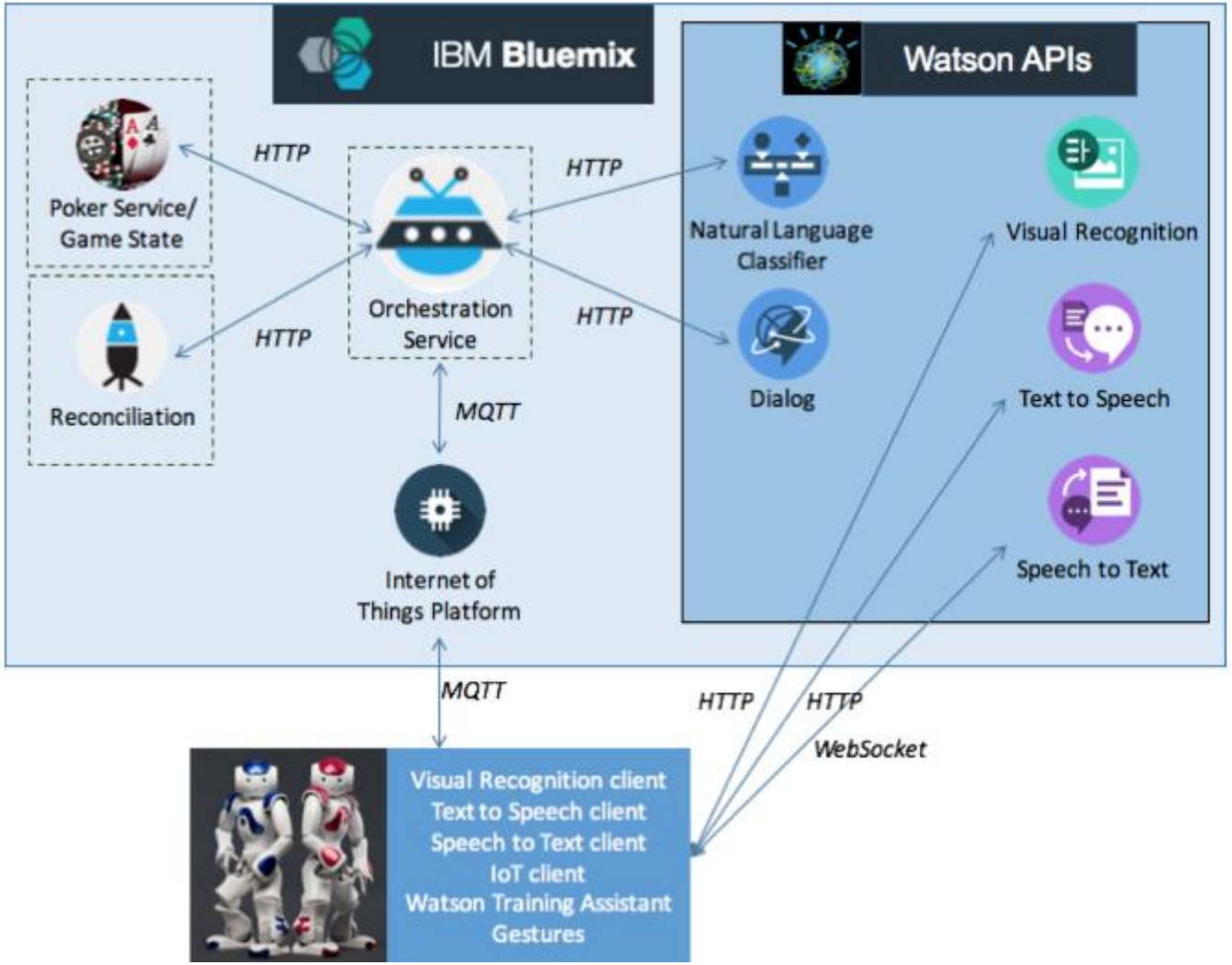
PE 581.948

- http://www.ninjamarketing.it/2017/02/17/caratteristiche-evoluzioni-potenzialita-blockchain-roberto-ferrari-chebanca/

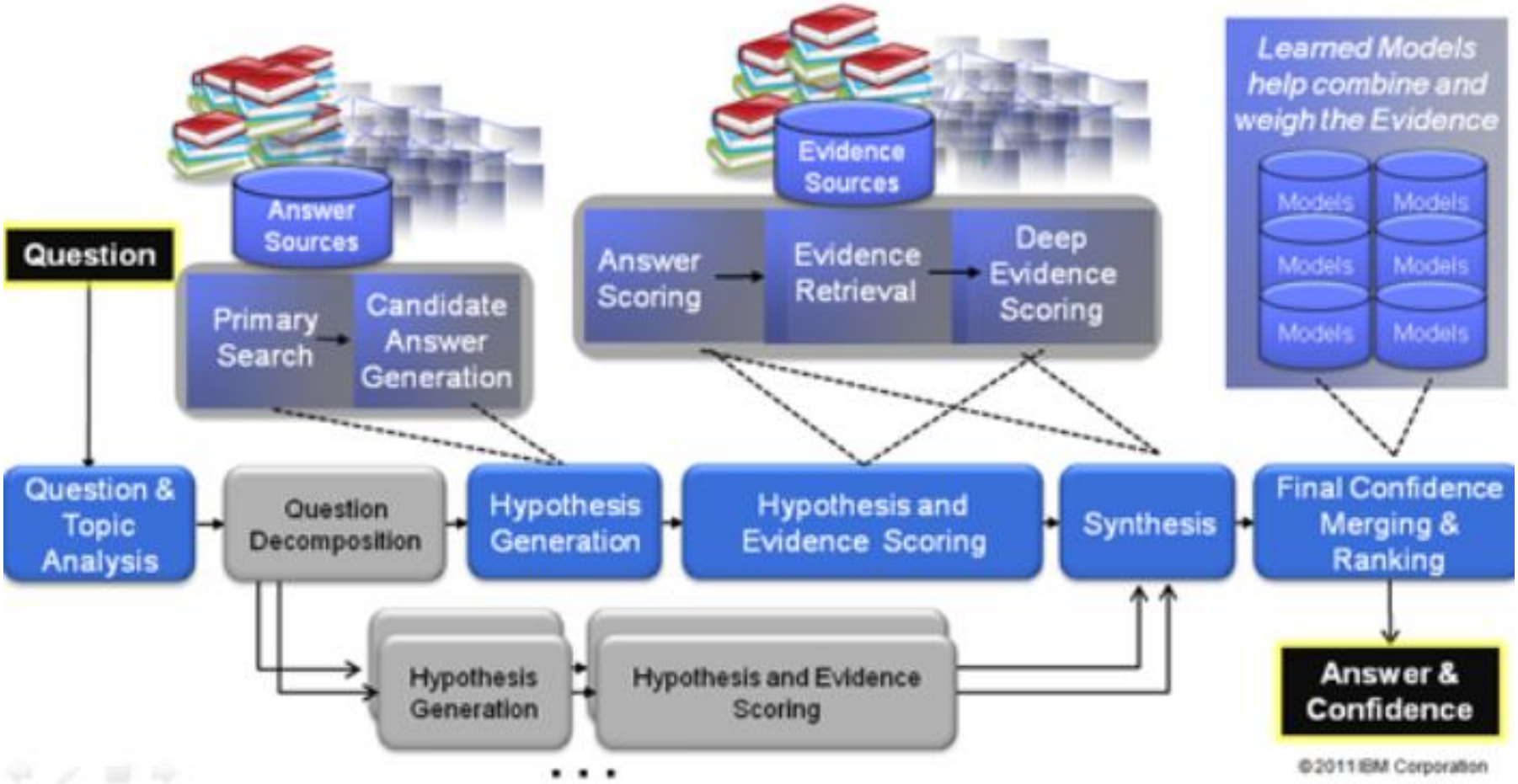
ALCUNI CASI DI USO DI AI NELLA SANITÀ

IBM- WATSON PER I DATI SANITARI ITALIANI

Architettura



DeepQ&A architecture



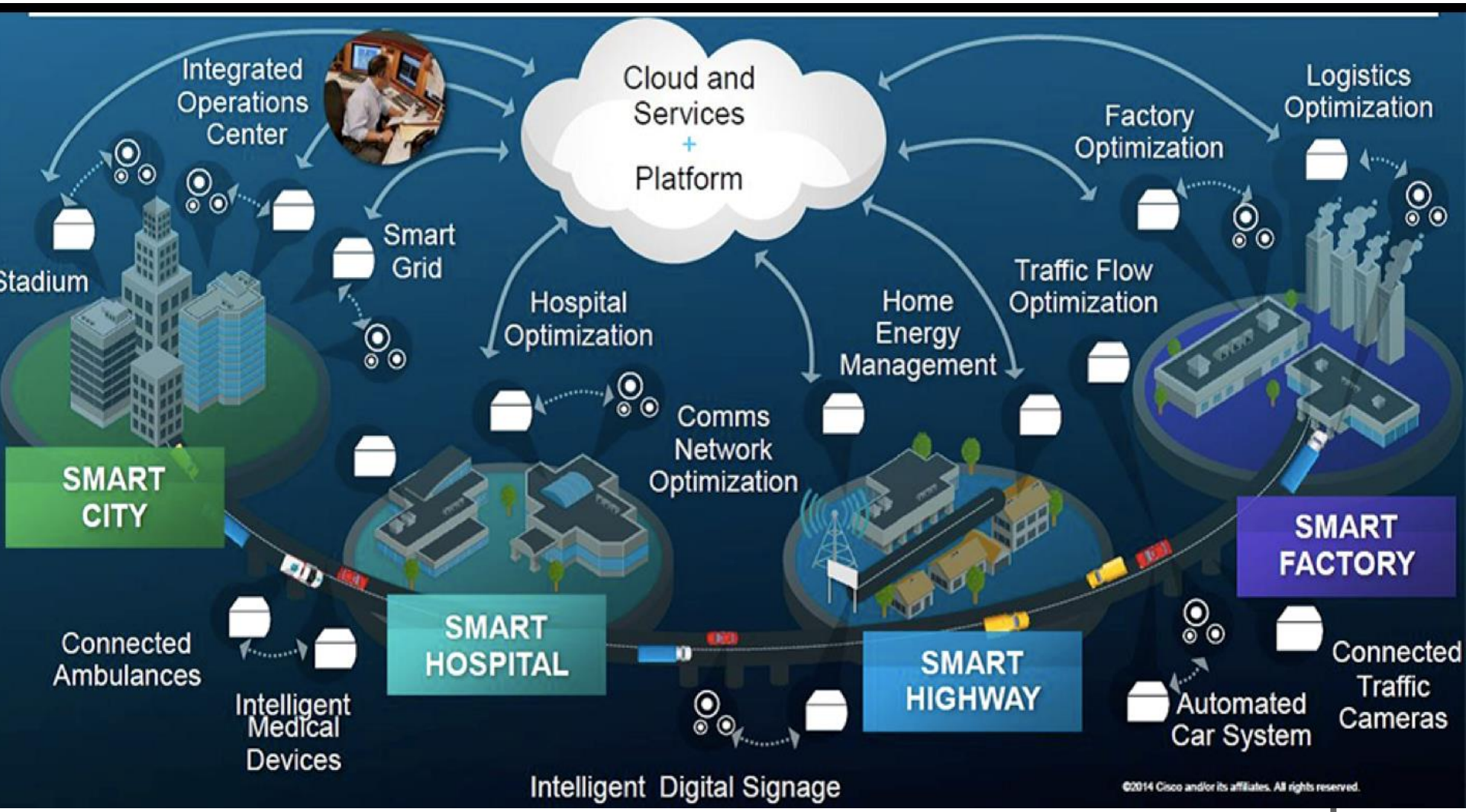
Investimento 150 milioni di dollari

- http://www.privacyitalia.eu/privacy-dati-sanitari-degli-italiani-regalati-ibm/2431/

Ma il Garante della privacy, **Antonello Soro**, già il 22 febbraio 2017 ha inviato una lettera a Governo e Regione Lombardia per avere chiarimenti sulla vicenda. Il Garante ha ribadito due concetti fondamentali per il rispetto della privacy dei cittadini italiani:

- I trattamenti di dati sanitari per fini di ricerca medica, biomedica ed epidemiologica possono prescindere dal consenso dell'interessato **solo quando la ricerca sia prevista da un'espressa disposizione di legge.**
- Possono trattare dati personali solo *"soggetti appositamente designati responsabili esterni del trattamento, individuati tra soggetti che, per esperienza, capacità e affidabilità, forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni".*

Cloud+Geolocalization



DEEPMIND (GOOGLE) E NHS-UK

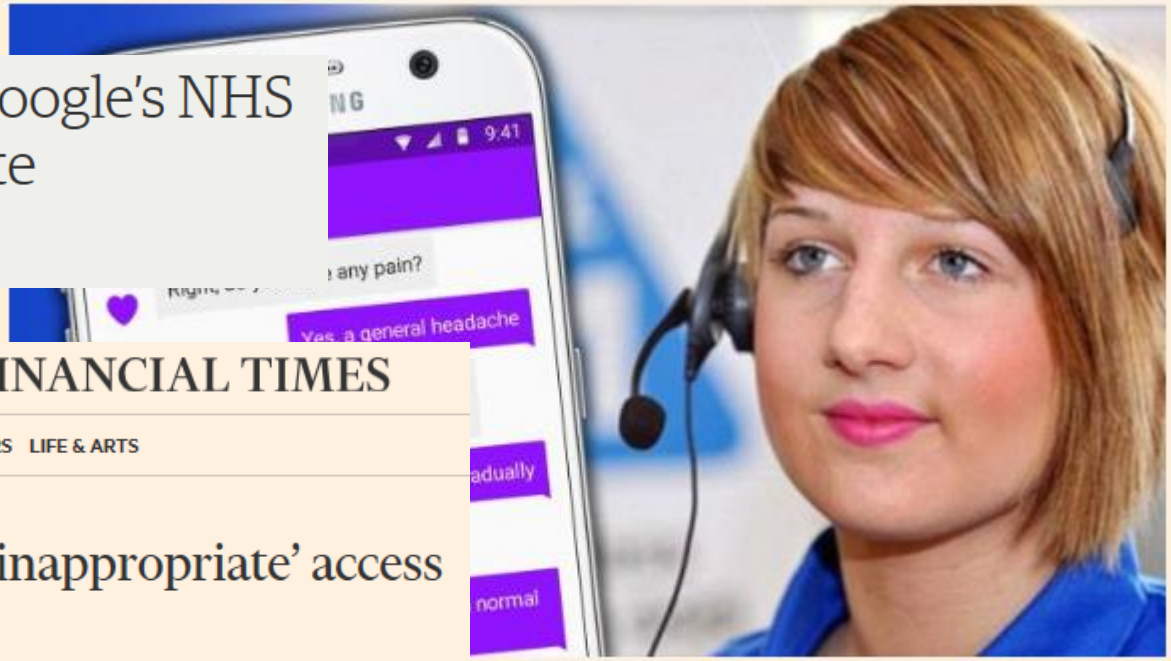
FINANCIAL TIMES

WORLD US COMPANIES MARKETS OPINION WORK & CAREERS LIFE & ARTS

National Health Service + Add to myFT

NHS to trial artificial intelligence app in place of 111 helpline

London experiment will perform triage for urgent but non-life-threatening conditions



on a phone app, like the one already built by Babylon, rather than
ıfage; company; NHS

The Guardian view on Google's NHS grab: legally inappropriate

Editorial

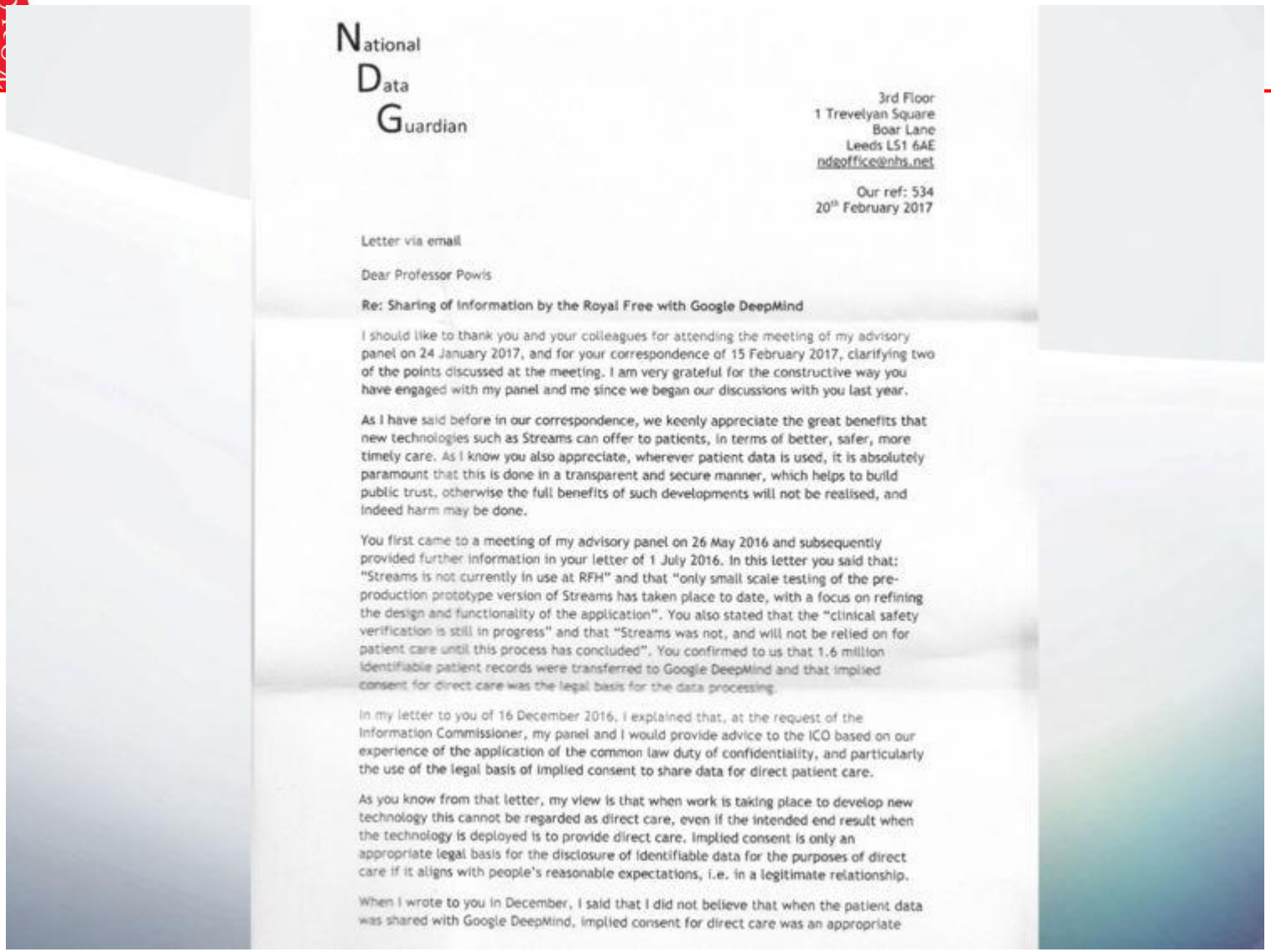
FINANCIAL TIMES

HOME WORLD US COMPANIES MARKETS OPINION WORK & CAREERS LIFE & ARTS

Data protection + Add to myFT

DeepMind given 'legally inappropriate' access to NHS data

Records were shared with the Google-owned AI company to trial Streams health



National
Data
Guardian

3rd Floor
1 Trevelyan Square
Boar Lane
Leeds LS1 6AE
ndgoffice@nhs.net

Our ref: 534
20th February 2017

Letter via email

Dear Professor Powis

Re: Sharing of information by the Royal Free with Google DeepMind

I should like to thank you and your colleagues for attending the meeting of my advisory panel on 24 January 2017, and for your correspondence of 15 February 2017, clarifying two of the points discussed at the meeting. I am very grateful for the constructive way you have engaged with my panel and me since we began our discussions with you last year.

As I have said before in our correspondence, we keenly appreciate the great benefits that new technologies such as Streams can offer to patients, in terms of better, safer, more timely care. As I know you also appreciate, wherever patient data is used, it is absolutely paramount that this is done in a transparent and secure manner, which helps to build public trust, otherwise the full benefits of such developments will not be realised, and indeed harm may be done.

You first came to a meeting of my advisory panel on 26 May 2016 and subsequently provided further information in your letter of 1 July 2016. In this letter you said that: "Streams is not currently in use at RFH" and that "only small scale testing of the pre-production prototype version of Streams has taken place to date, with a focus on refining the design and functionality of the application". You also stated that the "clinical safety verification is still in progress" and that "Streams was not, and will not be relied on for patient care until this process has concluded". You confirmed to us that 1.6 million identifiable patient records were transferred to Google DeepMind and that implied consent for direct care was the legal basis for the data processing.

In my letter to you of 16 December 2016, I explained that, at the request of the Information Commissioner, my panel and I would provide advice to the ICO based on our experience of the application of the common law duty of confidentiality, and particularly the use of the legal basis of implied consent to share data for direct patient care.

As you know from that letter, my view is that when work is taking place to develop new technology this cannot be regarded as direct care, even if the intended end result when the technology is deployed is to provide direct care. Implied consent is only an appropriate legal basis for the disclosure of identifiable data for the purposes of direct care if it aligns with people's reasonable expectations, i.e. in a legitimate relationship.

When I wrote to you in December, I said that I did not believe that when the patient data was shared with Google DeepMind, implied consent for direct care was an appropriate

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA
CAMPUS DI RAVENNA

Monica Palmirani
CIRSFID, Università di Bologna
monica.palmirani@unibo.it
www.unibo.it