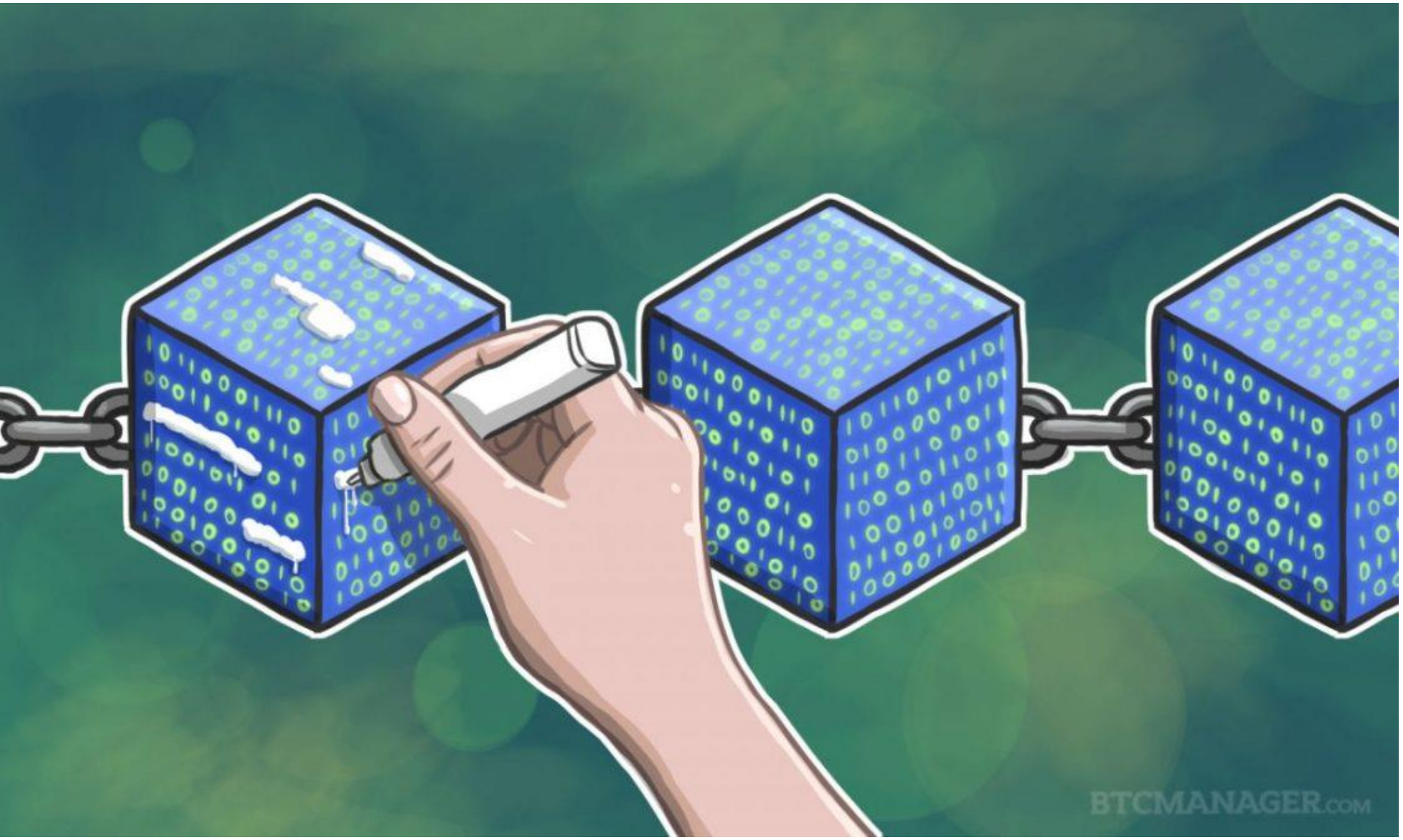
Blockchain

Fondamenti e applicazioni

AzzurroDigitale
STRATEGY&VENTURES

BLOCKCHAIN: la necessità di condividere dati immutabili



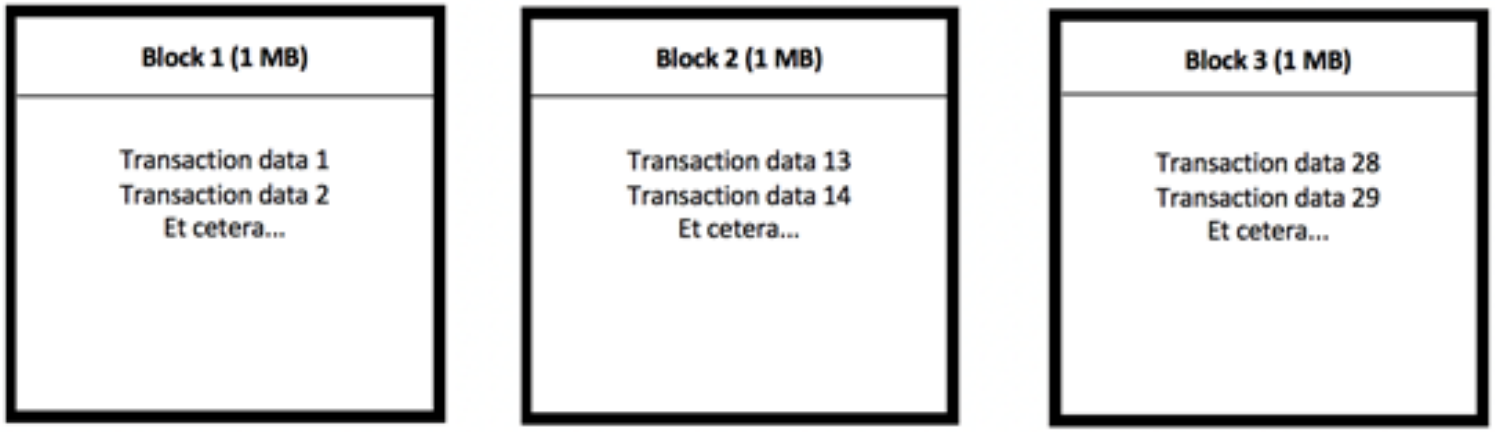
Perché è così importante poter condividere informazioni che nessuno possa alterare?

Pensate al fatto che un impiegato di banca con il giusto livello di accesso, potrebbe aggiungere o togliere zeri al vostro conto.

O al suo.

AzzurroDigitale
STRATEGY&VENTURES

BLOCKCHAIN: la necessità di condividere dati immutabili



Potrei prendere allora una lista di transazioni (o molto altro!) e condividerla con molti miei amici, colleghi o concittadini (peers).

E' sufficiente? E se uno si sveglia la mattina, cambia una cifra e decide che è ricco?

Per trovare l'errore non posso sfogliare un *ledger* di centinaia di GB!! Esiste un modo per verificare l'integrità guardando solo l'ultimo record?

AzzurroDigitale
STRATEGY&VENTURES

BLOCKCHAIN: come nasce?

La prima blockchain fu introdotta, nel 2008, ad opera di Satoshi Nakamoto[4] (pseudonimo di un autore la cui identità è tuttora sconosciuta), e implementata l'anno seguente, con l'obiettivo di fungere da *libro mastro* (registro di tutte le transazioni) della nascente valuta digitale Bitcoin.[5][2] Satoshi Nakamoto usava le parole *block* e *chain* in modo separato nell'articolo originale del 2008.[6] Nel 2009 la creazione di Satoshi Nakamoto, Bitcoin, fu utilizzata per la prima volta per l'acquisto di un bene fisico: una pizza.[7]

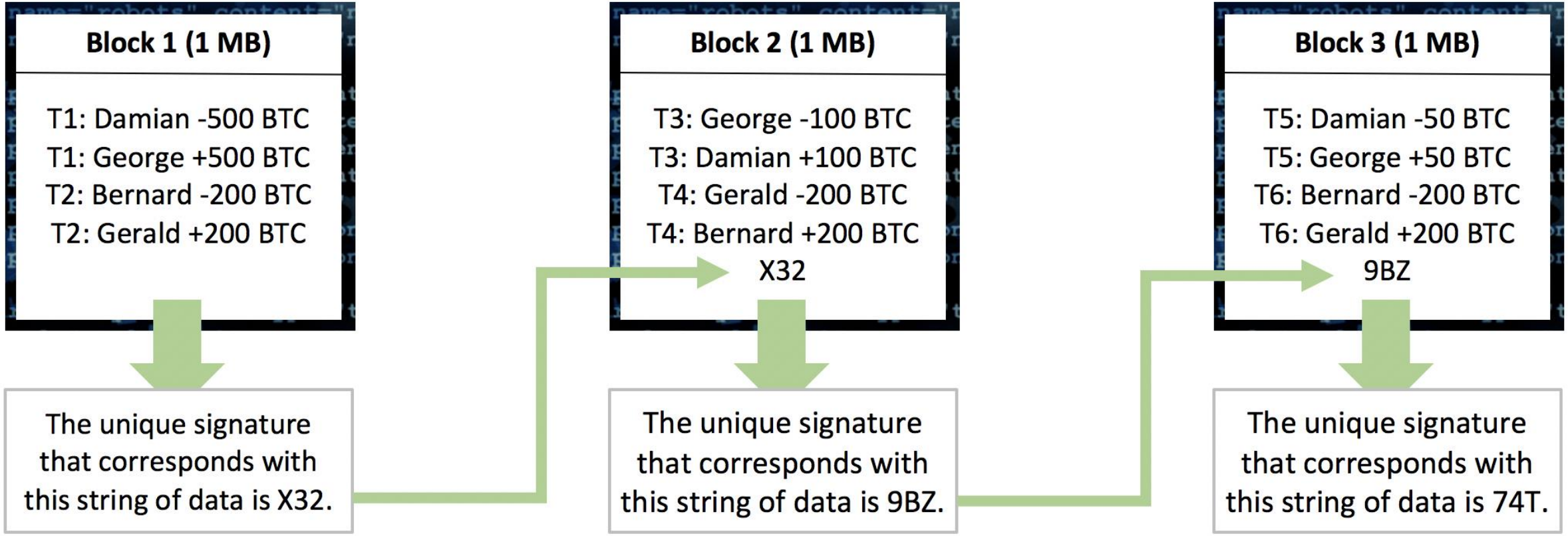
BLOCKCHAIN.COM Prodotti Dati Esploratore

hash	000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
conferme	628.257
timestamp	2009-01-03 19:15
Altezza	0
Minatore	Unknown
Numero di transazioni	1
Difficoltà	1,00
Radice di Merkle	4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

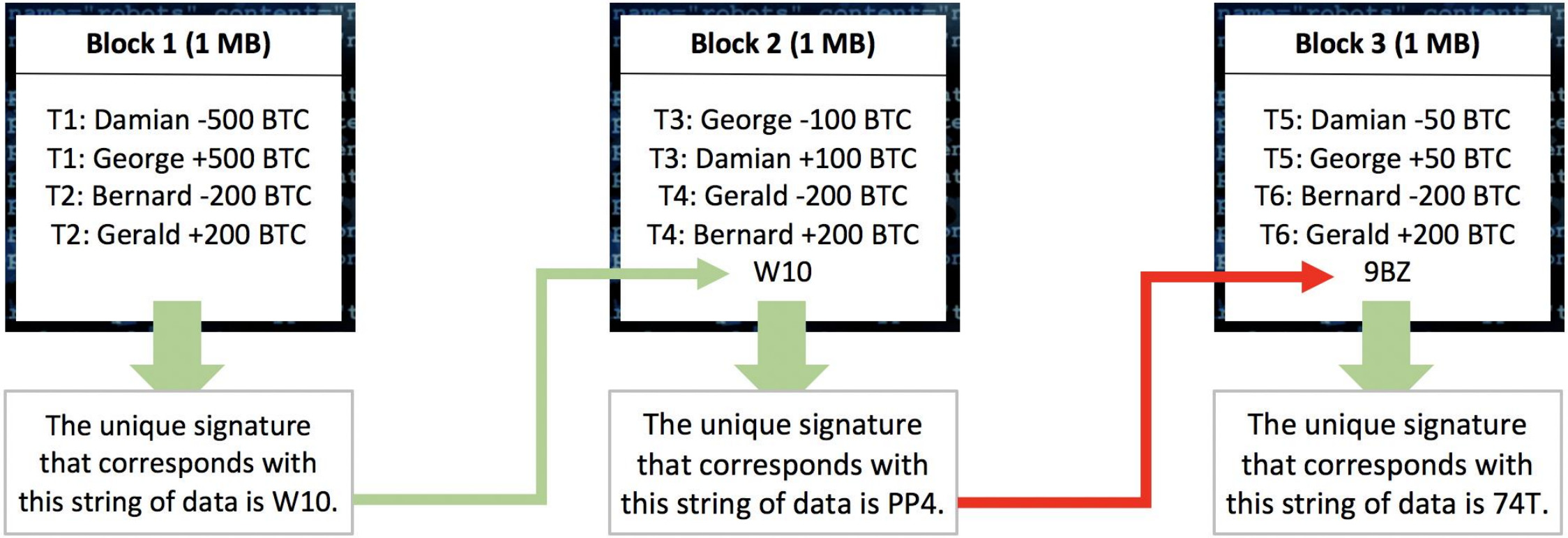
```
00000000 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000020 00 00 00 00 3B A3 ED FD 7A 7B 12 B2 7A C7 2C 3E ....;£íýz{.²zÇ,>
00000030 67 76 8F 61 7F C8 1B C3 88 8A 51 32 3A 9F B8 AA gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040 4B 1E 5E 4A 29 AB 5F 49 FF FF 00 1D 1D AC 2B 7C K.^J)«_Iÿÿ...¬+|
00000050 01 01 00 00 00 01 00 00 00 00 00 00 00 00 00 00 ................
00000060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000070 00 00 00 00 00 00 FF FF FF FF 4D 04 FF FF 00 1D ......ÿÿÿÿM.ÿÿ..
00000080 01 04 45 54 68 65 20 54 69 6D 65 73 20 30 33 2F ..EThe Times 03/
00000090 4A 61 6E 2F 32 30 30 39 20 43 68 61 6E 63 65 6C Jan/2009 Chancel
000000A0 6C 6F 72 20 6F 6E 20 62 72 69 6E 6B 20 6F 66 20 lor on brink of
000000B0 73 65 63 6F 6E 64 20 62 61 69 6C 6F 75 74 20 66 second bailout f
000000C0 6F 72 20 62 61 6E 6B 73 FF FF FF FF 01 00 F2 05 or banksÿÿÿÿ..ò.
000000D0 2A 01 00 00 00 43 41 04 67 8A FD B0 FE 55 48 27 *....CA.gŠý°þUH'
000000E0 19 67 F1 A6 71 30 B7 10 5C D6 A8 28 E0 39 09 A6 .gñ¦q0·.\Ö¨(à9.¦
000000F0 79 62 E0 EA 1F 61 DE B6 49 F6 BC 3F 4C EF 38 C4 ybàê.aÞ¶Iö¼?Lï8Ä
00000100 F3 55 04 E5 1E C1 12 DE 5C 38 4D F7 BA 0B 8D 57 óU.å.Á.Þ\8M÷°..W
00000110 8A 4C 70 2B 6B F1 1D 5F AC 00 00 00 00 ŠLp+kñ._¬....
```

AzzurroDigitale
STRATEGY&VENTURES

BLOCKCHAIN: come è fatta?

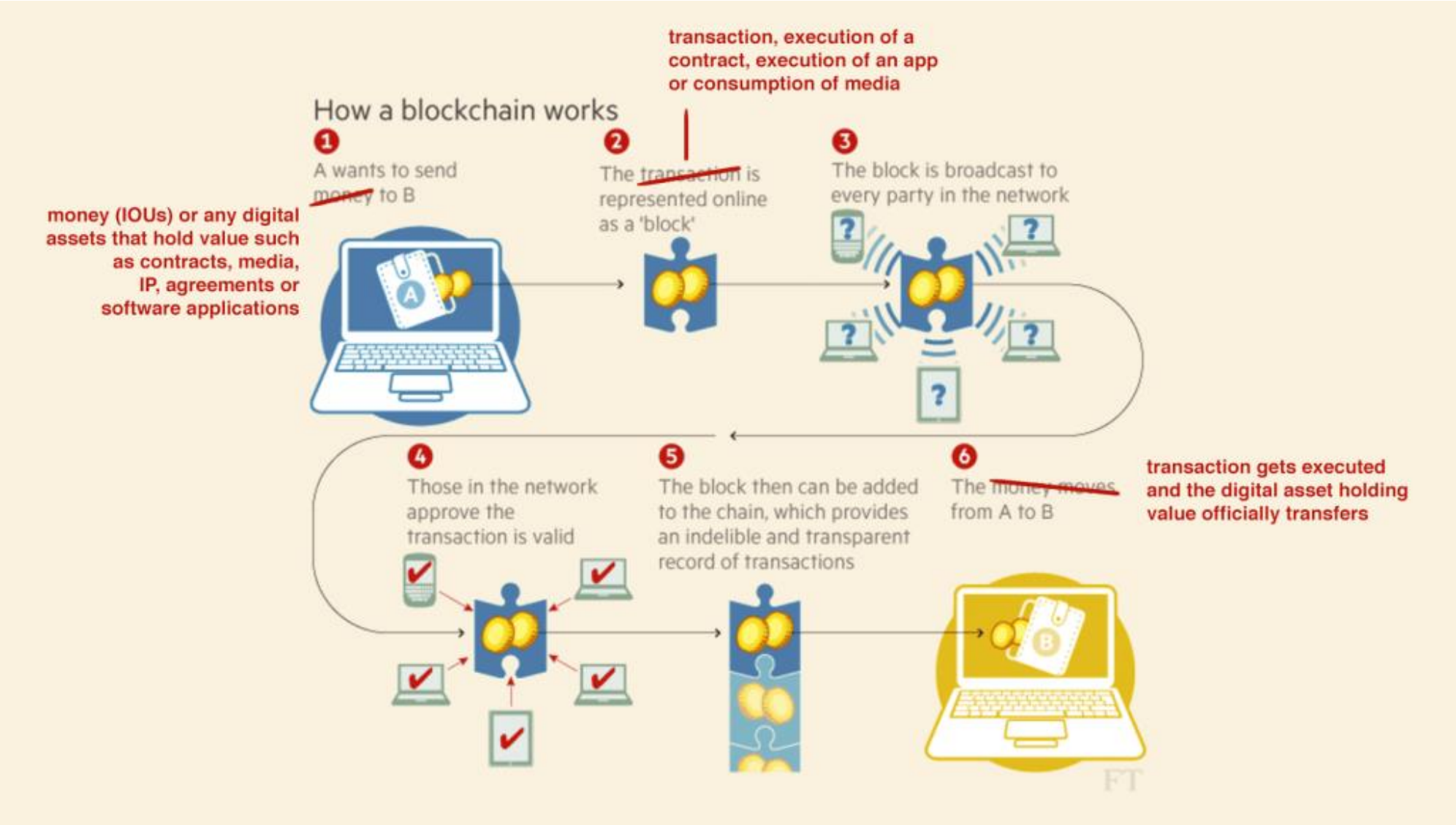


BLOCKCHAIN: cosa accade se tento di manometterla?



AzzurroDigitale
STRATEGY&VENTURES

BLOCKCHAIN: come aggiungo un «asset» alla blockchain?



AzzurroDigitale
STRATEGY&VENTURES

BLOCKCHAIN: i benefici

Benefits Of Blockchain Technology

Immutable data
All information stored on the blockchain is permanent and unable to be changed.

Digital Freedom
Blockchains are decentralized. There is no organized company controlling the information stored on them how they operate.

Anonymity & Privacy
Cryptocurrencies built on top of blockchain technology gives individuals the capability to carry out transactions anonymously.

Security
Public blockchains are distributed across hundreds of thousands of computers. It would be impossible to attack every simultaneously.

No more intermediaries
Banks, Paypal, Visa, and WesternUnion are all examples of intermediaries. Customers rely on them to facilitate monetary transactions.

Lower Transaction Fees
Users can transfer millions of dollars worth on blockchain networks for less than $1.00.

CryptoManiaks
Master the Crypto World

AzzurroDigitale
STRATEGY&VENTURES

BLOCKCHAIN: ne parlano tutti!

AzzurroDigitale
STRATEGY&VENTURES

Record keeping: storage of static information

Transactions: registry of tradeable information

1 Static registry

- Distributed database for storing reference data

Example

- Land title
- Food safety and origin
- Patent

2 Identity

- Distributed database with identity-related information
- Particular case of static registry treated as a separate group of use cases due to extensive set of identity-specific use cases

Example

- Identity fraud
- Civil-registry and identity records
- Voting

3 Smart contracts

- Set of conditions recorded on a blockchain triggering automated, self-executing actions when these predefined conditions are met

Example

- Insurance-claim payout
- Cash-equity trading
- New-music release

4 Dynamic registry

- Dynamic distributed database that updates as assets are exchanged on the digital platform

Example

- Fractional investing
- Drug supply chain

5 Payments infrastructure

- Dynamic distributed database that updates as cash or cryptocurrency payments are made among participants

Example

- Cross-border peer-to-peer payment
- Insurance claim

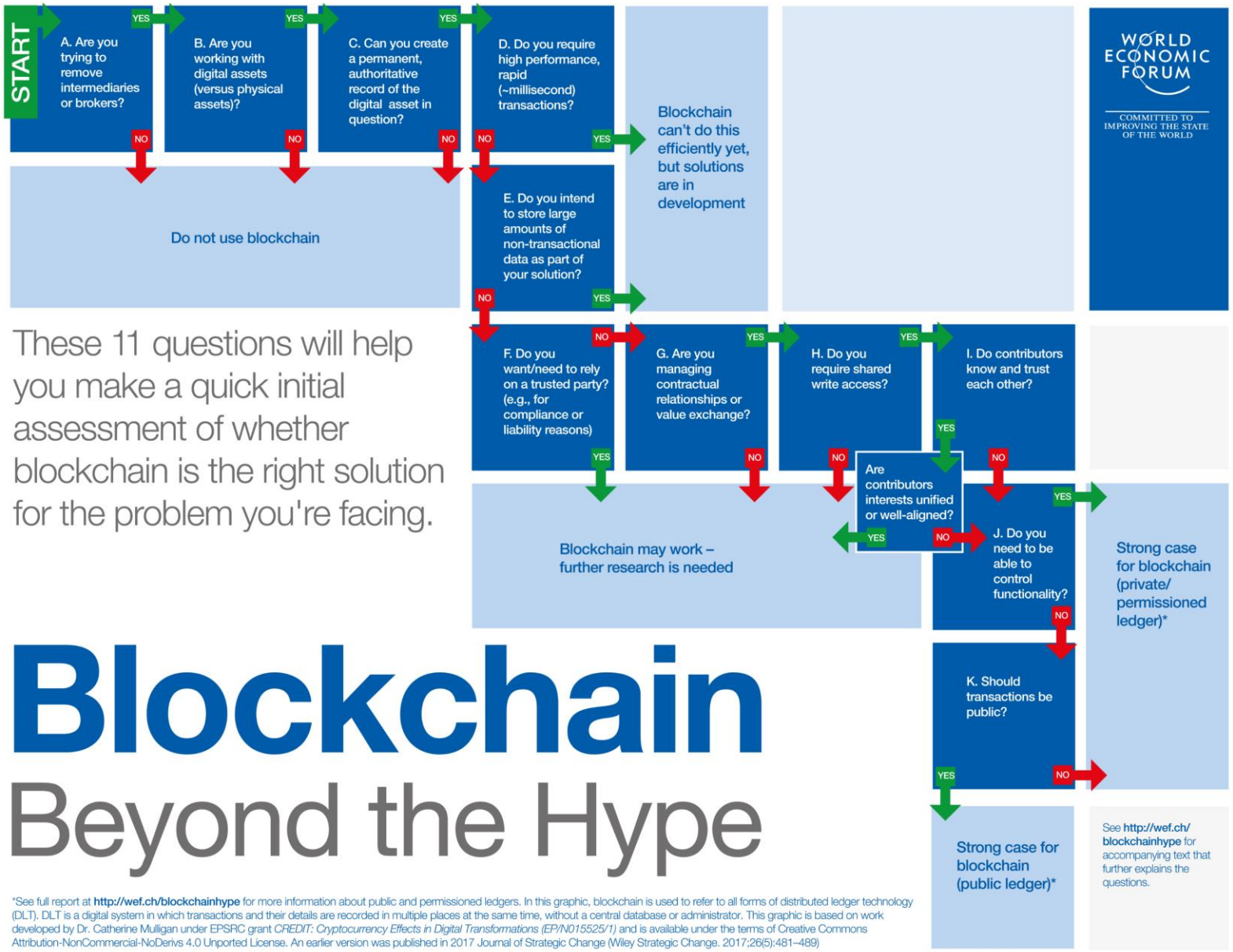
6 Other

- Use case composed of several of the previous groups
- Standalone use case not fitting any of the previous categories

Example

- Initial coin offering
- Blockchain as a service

BLOCKCHAIN: QUANDO mi serve una blockchain? Modello di Catherine Mulligan



Tracciare gli scambi di prodotti	in generale **NO**
Tracciare gli scambi di prodotti	in un consorzio **SI**
Gestire un registro amministrativo	**NO**
Salvare letteratura o beni artistici	**NO**
Registrare i controlli qualità su un prodotto	se nello stesso gruppo **SI**
Tracciare i beni in una catena produttiva	**SNI**
Convalidare i biglietti di un concerto	**NO**
Registrare un brevetto	**SI**

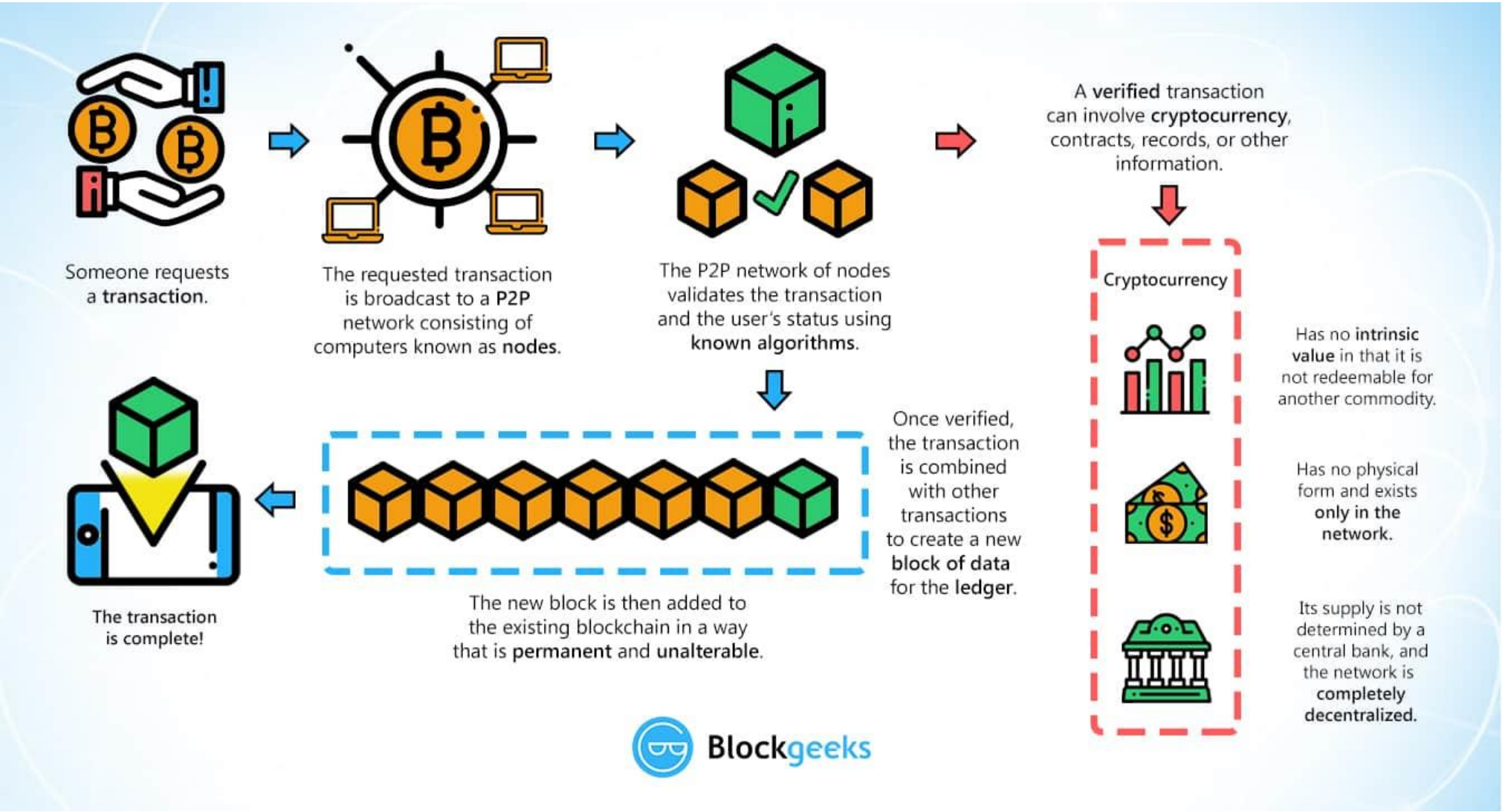
AzzurroDigitale STRATEGY&VENTURES

BLOCKCHAIN: QUANDO mi serve una blockchain?

Insomma, se nel fenomeno in analisi c’è un **NETWORK** la **BLOCKCHAIN** crea un grande **valore**.

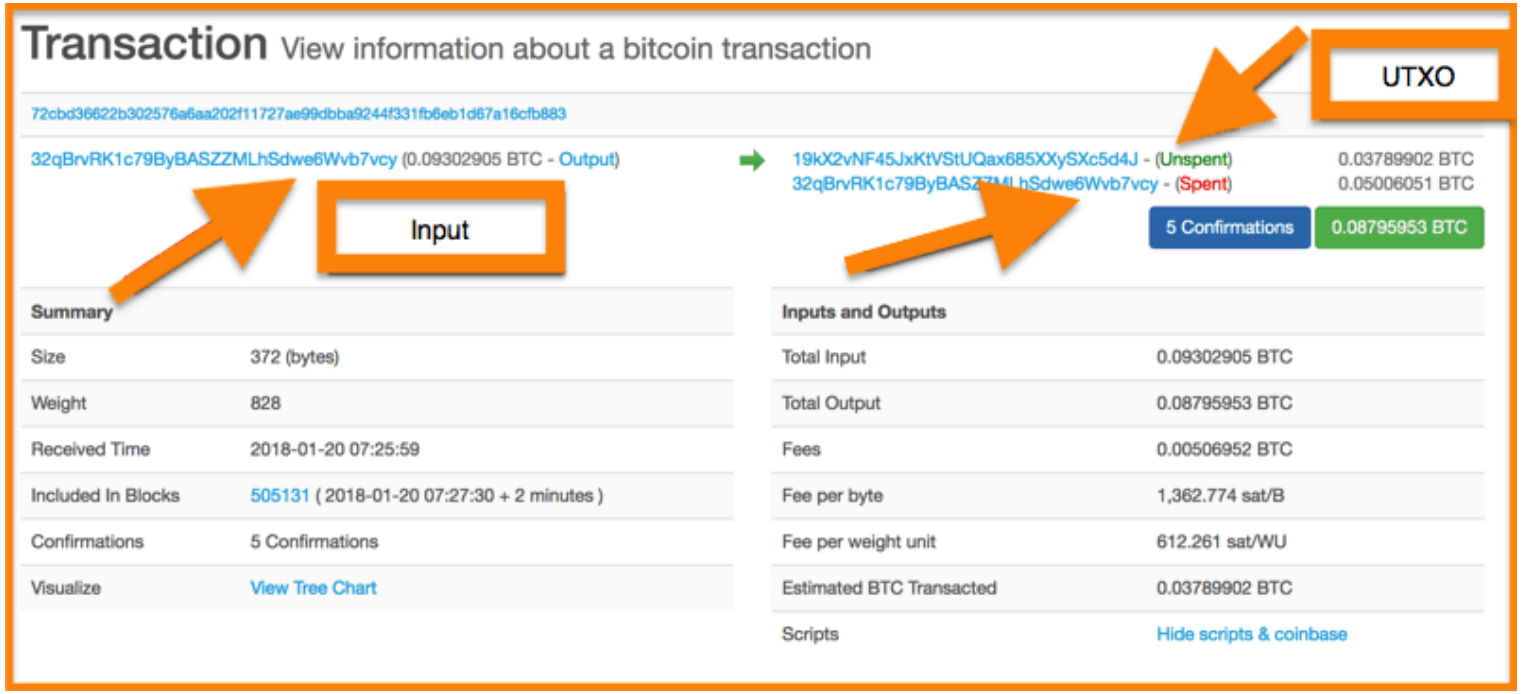
Se non c’è, si può fare poco…

BLOCKCHAIN: ok ma come posso usarla per scambiare valuta??



AzzurroDigitale
STRATEGY&VENTURES

BLOCKCHAIN: una transazione? Cioè? E la mia banca dove sta?



Qui si parla di **denaro**, ma potrebbero essere:

- **Materie** prime
- **Commodities**
- Prodotti **finanziari**
- **Servizi** digitali
- …

Alla fine il mio saldo in banca è una somma di accrediti, no?

La transazione avviene tra (almeno un) indirizzo di INPUT e

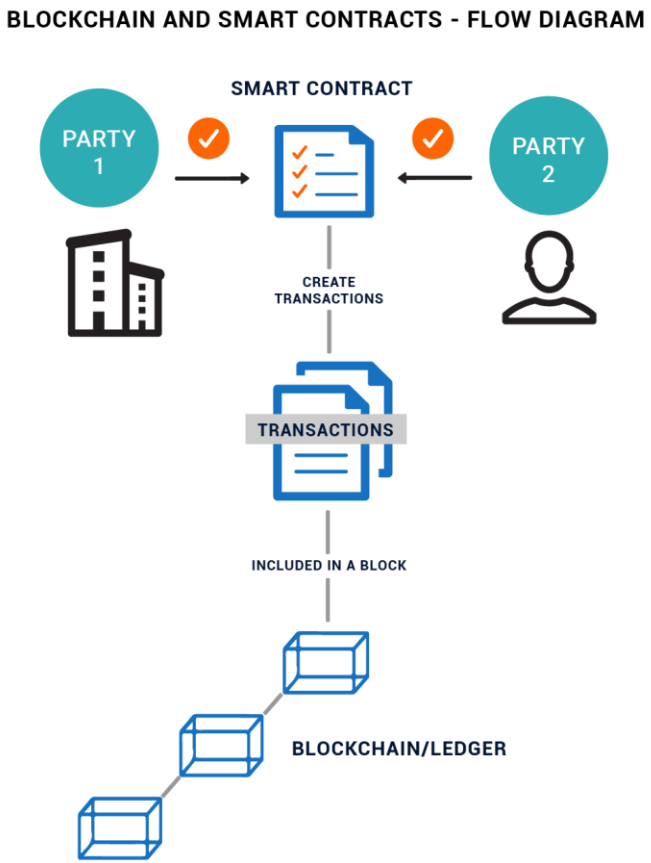
Ad ogni transazione, (almeno un) **INPUT** e consumato per generare una (o più di una) **SPESA** e un **RESTO** (UTXOs) e una **FEE** di transazione.

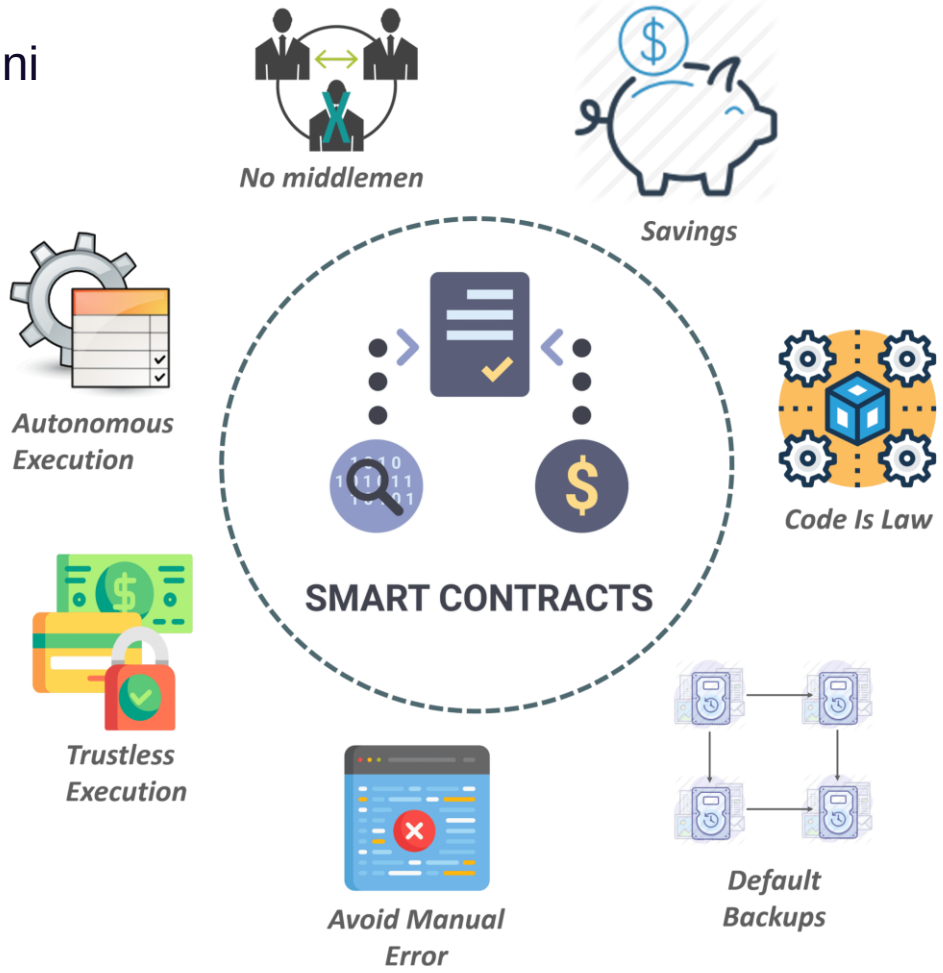
A chi si paga la **FEE**? Al nodo che ha permesso di registrare quella transazione!

AzzurroDigitale
STRATEGY&VENTURES

BLOCKCHAIN: posso anche automatizzare le transazioni

La blockchain può contenere qualsiasi asset digitale (*leggero). Se io mettessi del codice macchina, che consente di validare la legittimità di una transazione, o di scaturirne una?

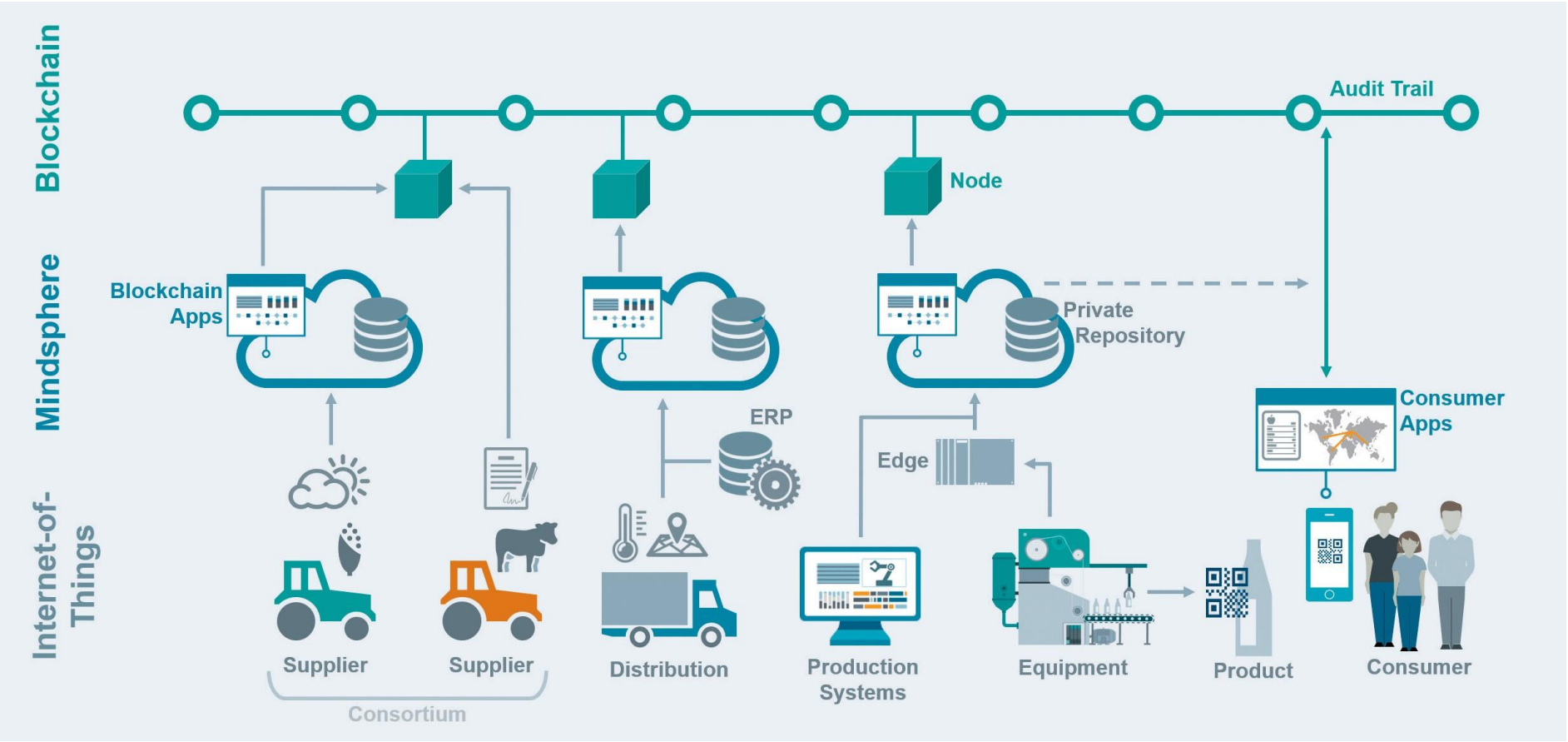




Il contratto (o la sottoscrizione di quest'ultimo) è salvata nella blockchain, quindi nessuno può tirarsi indietro, né rifiutarsi di pagare!

AzzurroDigitale
STRATEGY&VENTURES

BLOCKCHAIN: un esempio sulla tracciabilità della supply chain (SIEMENS)



- **Chi** ha prodotto il latte che bevo?
- **Quando**?
- Che alimentazione ha ricevuto l'animale che lo ha prodotto?
- Se dovesse esserci un problema di qualità, come identifico la **responsabilità**?

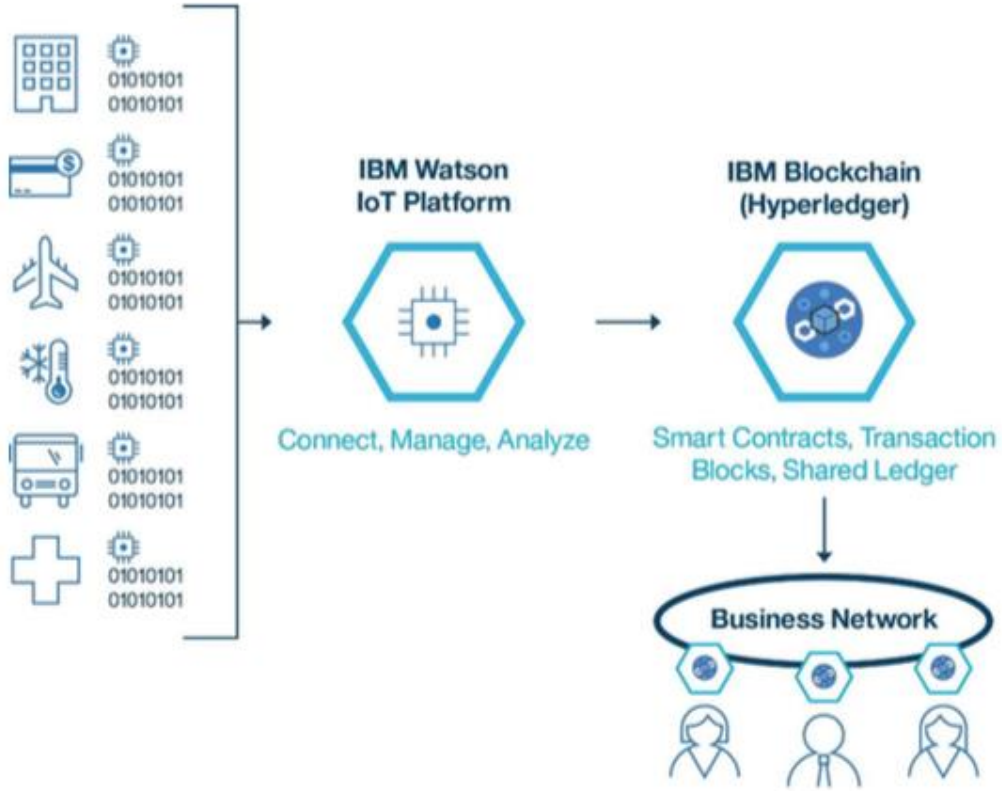
Perché non posso semplicemente annotare i dati su un **DB** trusted?
…perché con la **BLOCKCHAIN** posso invalidare un dato solo con l'omertà di tutti quelli che hanno usato blocchi successivi al mio.

AzzurroDigitale STRATEGY&VENTURES

BLOCKCHAIN: l’IoT e la blockchain

Posso usare un dispositivo **IoT** per scrivere dati sulla blockchain?

Si, ma… mi scontro con il tema della **notarizzazione**, ossia: l’IoT diventa il responsabile di certificare il dato. Quindi è necessario che il partner che certifica e installa l’IoT sia **trusted**.



La blockchain può garantire che un tale dato sia stato scritto, non la veridicità del dato in sé.

AzzurroDigitale
STRATEGY&VENTURES

BLOCKCHAIN: QUANDO mi serve una blockchain?

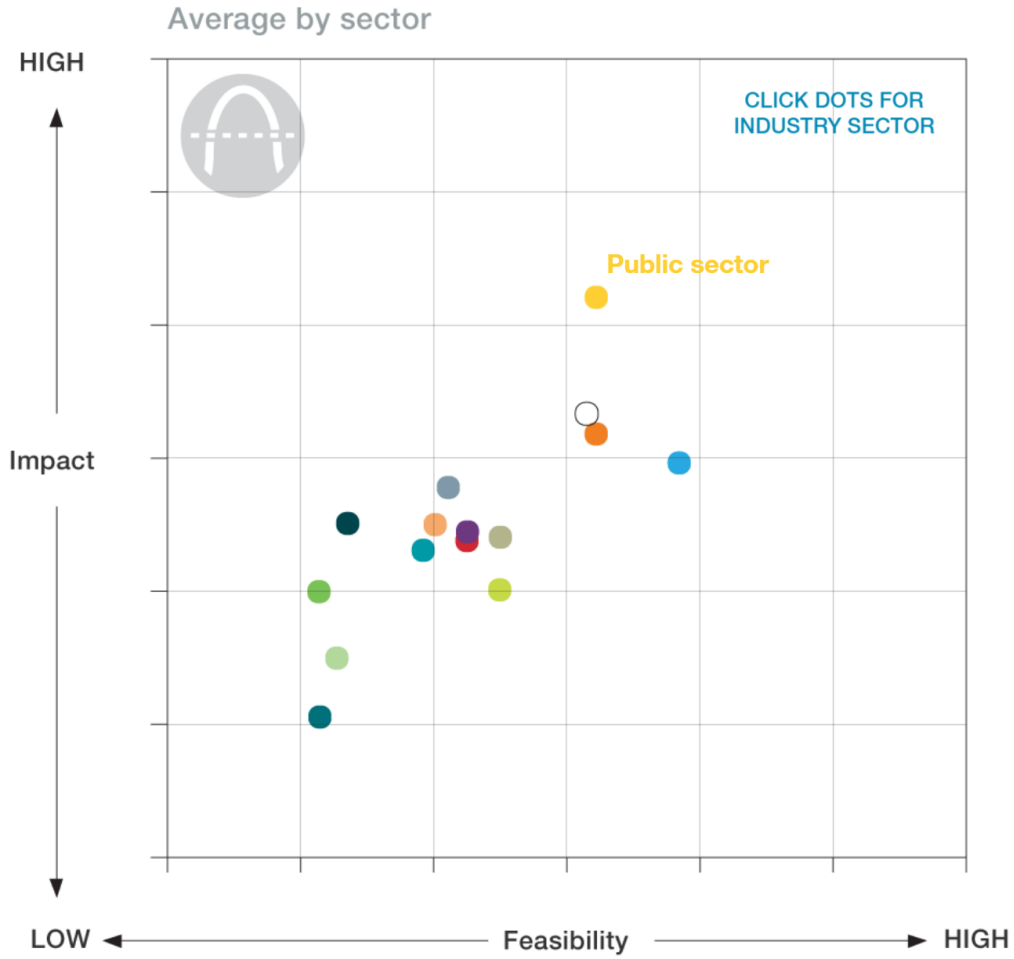
La blockchain è uno **strumento** che, nel contesto giusto, aumenta il **trust**.

I vantaggi in termini di valore, aggiunto dallo strumento, devono essere analizzati caso per caso e va capito se tutti i partecipanti al network ricevono **valore** sufficiente da questo strumento, tanto da decidere di adottarlo e **rispettarlo***.

BLOCKCHAIN: opportunities

https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/blockchain-explained-what-it-is-and-isnt-and-why-it-matters

Blockchain opportunities by industrial sector



CLICK ON INDUSTRY SECTOR TO SEE PRIORITIZATION FOR THAT INDUSTRY

- Overall average
- Agriculture
- Arts and recreation
- Automotive
- Financial services
- Healthcare
- Insurance
- Manufacturing
- Mining
- Property
- Public sector
- Retail
- Technology, media, and telecom
- Transport and logistics
- Utilities

McKinsey&Company

AzzurroDigitale STRATEGY&VENTURES

Grazie

AzzurroDigitale
STRATEGY&VENTURES

Via della Croce Rossa, 42
35129 - Padova

BLOCKCHAIN: fluttuazione BITCOIN con il COVID-19

Published on TradingView.com, April 30, 2020 05:05:29 EST
KRAKEN:XBTEUR, 240 8038.8 ▼ −36.1 (−0.45%) **O:**8455.1 **H:**8497.0 **L:**7858.9 **C:**8038.8

AzzurroDigitale
STRATEGY&VENTURES

BLOCKCHAIN: la Proof-Of-Work (POW)

Block 5 (1 MB)

Transaction data

+ Signature block 4

+ Random nonce: p##@1

Hashes to signature:
0000000P3X22A

Block 6 (1 MB)

Transaction data

+ 0000000P3X22A

+ Random nonce: p##@1

Hashes to signature:
0000000112LLK4

Block 7 (1 MB)

Transaction data

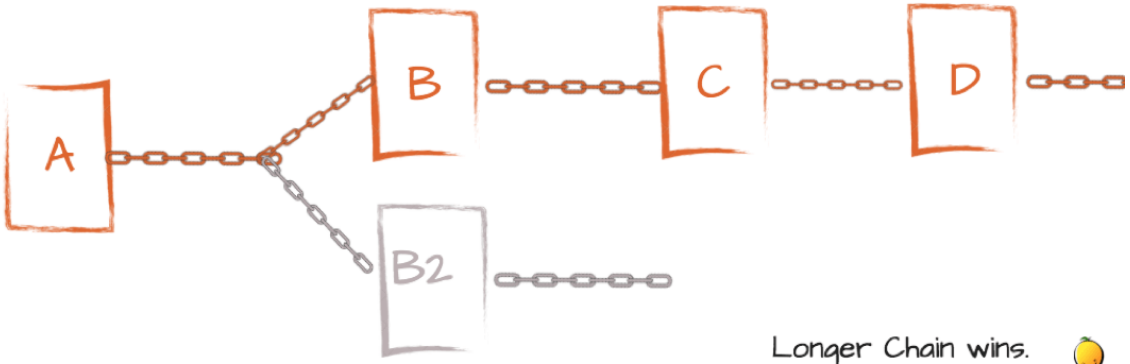
+ 0000000112LLK4

+ Random nonce: (???)

Hash needs to start with at least seven consecutive zero's

Miners are spending electricity in the form of computational power in order to insert as many random nonces as fast as possible untill they find a nonce that, together with the rest of the block data, leads to hash output (signature) that starts with at least seven zero's.

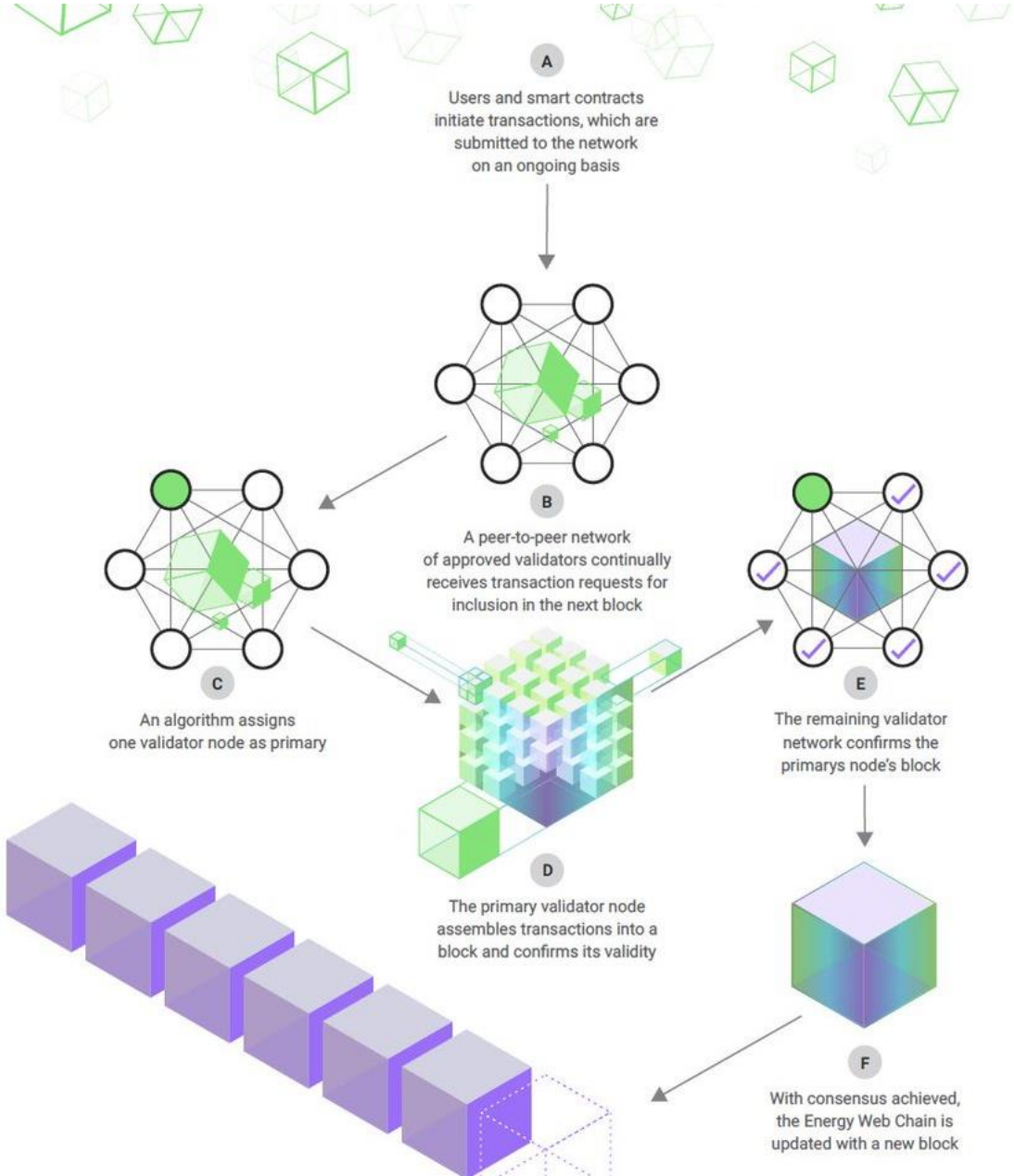
Lo scopo è rendere **COSTOSO** estendere la blockchain, in modo che i nodi desistano dal tentativo di biforcarla.



Longer Chain wins.
Shorter is "orphaned"

AzzurroDigitale
STRATEGY&VENTURES

BLOCKCHAIN: la Proof-Of-Autority



AzzurroDigitale
STRATEGY&VENTURES