BLOCKCHAIN

TAXONOMY

TIPOLOGIE, FUNZIONI, APPLICAZIONI

<HELLO WORLD>





● **info@blockchaincaffe.it**

● **https://www.blockchaincaffe.it**

● **https://www.youtube.com/c/BlockChainCaffe**

TL; DR / EXECUTIVE SUMMARY BLOCK OR NO-BLOCK 

THERE IS NO PRIVATE

BLOCKCHAIN

TAXONOMY

TUTTO QUELLO CHE AVRESTI SEMPRE VOLUTO SAPERE SUI TIPI DI

BLOCKCHAIN,

L’HAI CHIESTO, TI HANNO RISPOSTO, MA ERA SBAGLIATO

COME SPIEGARLO MALE

SEMPLIFICARE NON E’ BANALIZZARE

LA GRANDE DOMANDA



LA BRUTTA RISPOSTA



LA GRANDE CONFUSIONE?

… IN QUATTRO SALSE ...



… O TRE SALSE...



… O 4 CHE PERO’ SONO 3



VOCABOLARIO: NOT FOUND

**PERMISSIONED COST**

**IDENTIFIED OWNER**

**READ VALIDATE PERMISSIONLESS**

**IDENTITY**

**TRUSTED**

**WRITE**

**OWNERSHIP**

**FINALITY**

TASSONOMIA BINARIA

Divide le blockchain sulla base di **due** operazioni: **lettura e scrittura**

Per ogni operazione ammette **due** possibili valori: **tutti o “qualcuno”**

E’ APPLICABILE A QUALCOSA?



TASSONOMIA BINARIA

● Insufficiente per classificare **le viti** ! ● Non è una semplificazione

● E’ una **banalizzazione**

● Non è *“per far capire”*

● E’ per **vendere**

● **E’ sbagliata**

DA CAPO...



RIPARTIAMO DALLE BASI

DA DOVE PARTIAMO

DOVE VOGLIAMO ANDARE

PERCHE SIAMO QUI ?

SATOSHI NAKAMOTO

*“I've developed a new open source P2P e-cash system* 

*called Bitcoin. It's completely decentralized, with no*

*central server or trusted parties, because everything is*

*based on crypto proof instead of trust. Give it a try, or*

*take a look at the screenshots and design paper...”*

Posted by Satoshi Nakamoto on February 11, 2009 at 22:27

TUTTO QUESTO E’

DiSRuptive

LA BLOCKCHAIN



CARATTERISTICHE DI BITCOIN

● Pseudoanonimo ● Trustless

● Sicuro

● Decentralizzato ● Distribuito

● Libero, e gratuito\*

This is what you want +

Why you want it

● Non censurabile, inarrestabile ● Immutabile

● Scarso e limitato

COSA NON E’ LA BLOCKCHAIN

DA DOVE PARTIAMO

DOVE VOGLIAMO ANDARE

NON E’ FIDUCIA

La blockchain **vera** non chiede mai **fiducia** in nessuna forma. Tutto è **verificabile** in modo **autonomo** e diretto, tutto è **conoscibile**, quindi si elimina alla base la necessità di fidarsi di qualcuno/qualcosa

NON E’ FILE SHARING

I file non sono mai caricati in Blockchain per essere condivisi (salvo rarissimi casi) 

Lo scopo non è condividere informazioni 1:1

Per quello **c’è la mail**...

NON E’ CYBERSECURITY

Crittografia e sicurezza sono alla base della blockchain, ma non si fa sicurezza con la blockchain 

**NB:** le blockchain **pubbliche** sono immuni da **ransomware**...

NON E’ UN DATABASE

La blockchain è cara (€/byte), non indicizza tutti i dati, non permette di fare ricerche “SQL-like” 

**NB:** la blockchain **pubblica** ha altre caratteristiche che sono molto più di un DB

IL SENSO DELLA BLOCKCHAIN

**Avere un sistema di registrazione delle informazioni trasparente, verificabile in modo indipendente da terzi, non corruttibile, dimostrabilmente non soggetto ad ingerenze, forzature o specifici interessi, che registri le informazioni, i passaggi di stato delle stesse in ordine temporale, gli attori che hanno operato su di esse.**

BLOCKCHAIN STATE OF MIND

**CENTRALIZZATO**

**DECENTRALIZZATO**

**FIDUCIA**

**PRIVATO**

**PROPRIETARIO**

**CONDIVISO DISTRIBUITO**

**PUBBLICO**

**GLOBALE**

**LOCALIZZATO**

**AUTORIZZATO**

**TRASPARENTE**

**PERMISSIONLESS**

**VALUE**

**PROPOSITION**

**BUSINESS MODEL**

TUTTO QUESTO… SPAVENTA



RICERCARE ALTERNATIVE “COMODE”

● Mantenere il **”controllo”** sui dati

● Mantenere i dati **privati**

● Timore che Publicco = Chaos

● *“Si dice”* che la Blockchain non sia **GDPR** compliant ● Volontà di poter **cambiare** i dati

● Volontà di **avere il possesso** della piattaforma ● … perchè *“si pensa”* che sia più **sicuro**

L’ALTERNATIVA C’E’ ….

● Mantenere il **”controllo”** sui dati ● Mantenere i dati **privati** 

● Timore che Publicco = Chaos ● *“Si dice”* non sia **GDPR** compliant ● Volontà di poter **cambiare** i dati ● Volontà di **possesso** della piattaforma ● … perchè *“si pensa”* che sia più **sicuro**

DOVE C’E’ DOMANDA…



PUBBLICO vs PRIVATO

**PUBBLICHE:**

~~Lente~~ (Ligthning, Polygon etc)

Open/Permissionless

**GRANDI** (10K+ nodi)

**Trustless**

**Immutabili**

**Sicure** x 2000 milioni $ (2021Q2) TCO : molto basso

Affidabile ed **Autorevole** x Tutti

*...ma sembra “da nerd”*

**PRIVATE:**

Veloci

Chiuse/Permissioned

**Piccole** (1000 nodi MAX)

Necessitano **Fiducia**

Nessuna Garanzia solida (CRUD!) -???-

TCO : medio/alta

Riferimento Interno (al più) *..ma “sembra professional”*

QUAL’E’ QUELLA “VERA” ?

**PUBLICCA / VERA**

*****la Stele di Rosetta*

**PRIVATA / FINTA**

*****un post-it scritto con una penna estremamante costosa*

PUBBLICO vs PRIVATO

 Verifica autonoma

 Disintermediazione

 Inalterabilità del Dato

 Replicazione del Dato

 Crittografia a chiave pubblica  Condivisione\*

 Data Certa

 Decentralizzazione

 Trasparenza\*

 Tracciabilità

 Automazione

**\*\*** 

 **\*** *su quello che vuoi tu !* ***\*\**** *esclusi costi x* ***formazione*** *e transazioni*

I PROBLEMI DELLE PRIVATE

DAVVERO LE PRIVATE SONO COSI’ MESSE MALE O SEI UN SITH?

COS’E’ IL CONSENSO

“Un procedimento **decisionale collettivo** in cui un gruppo **converge** su una decisione e la supporta nel migliore interesse **del gruppo”**

“Un meccanismo **resiliente** usato in **reti** di computer per ottenere l’accordo su uno specifico valore di un dato o sullo **stato della rete** tra processi **distribuiti** o **attori multipli**”

NETWORK NIGHTMARE

● Nodi Offline 

● Nodi Off-on-off 

● Connessioni Instabili

● Dati corrotti

● Messaggi corrotti

● Nodi dell’Impero

● … e il Lato Oscuro

BIZANTINE SIEGE



BIZANTINE SIEGE

LA SOLUZIONE : POW

NON C’E’ NESSUN PUZZLE DA RISOLVERE

COSA FA IL MINER

● **Raccoglie nuove transazioni** 

● **Valida le transazioni**

● **Applica circa altri 40 controlli**

● **Esegue la “Proof of Work”**

● **Trova il “NONCE” giusto**

● **Chiude il blocco**

● **Lo aggiunge alla Blockchain**

● **Ricevere una ricompensa**

I PROBLEMI DELLE PRIVATE

DAVVERO LE PRIVATE SONO COSI’ MESSE MALE O SEI UN SITH?

“BLOCKCHAIN” PRIVATE

● Sicurezza Perimetrale 

● Validatori noti e scelti

● No consensus → **Ordinamento** ● **No BTF: *f*=1**

● **No transparenza, immutabilità** ● No cryptocoins (not a feature)

Ex: R3 Corda

**NO** 

**“BLOCK CHAIN” because**

**we don’t**

**need one”**

Ex: HYPERLEDGER



Ex: HYPERLEDGER – CASO 1



Ex: HYPERLEDGER – CASO 2



GAME OVER



CASI D’USO PER LE PRIVATE?

“I’M NOT COMPLETELY USELESS, I CAN BE USED AS A BAD EXAMPLE”

STALLO ALLA MESSICANA



E I GUAI DELLE PUBBLICHE ?

“E’ LA STAMPA BELLEZZA...”

LENTEZZA E SCALABILITA



LENTEZZA E SCALABILITA

POW E CONSUMO DI ENERGIA

https://www.cbeci.org

POW E CONSUMO DI ENERGIA

https://www.cbeci.org

E LA CRIMINALITA’?

Morell’s latest paper where he reaches two 

conclusions: first, that concerns about the

use of bitcoin in illicit finance are

exaggerated significantly, and second, that

blockchain analysis is very effective in

crime-fighting and intelligence

https://cryptoforinnovation.org/resources/Analysis\_of\_Bitcoin\_in\_Illicit\_Finance.pdf

MORALE ? JOIN THE REPUBLIC

GRAZIE !! 

info@blockchaincaffe.it