

manuale

BLOCKCHAIN PER IL BUSINESS

modelli di valutazione
e metodologie di progetto

Paolo Alessandroni

Manuale: Blockchain per il Business

Modelli di valutazione e Metodologie di progetto

Paolo Alessandroni

QUANDO LE FORMICHE SI METTONO
D'ACCORDO SPOSTANO L'ELEFANTE

PRIMA EDIZIONE MAGGIO 2019 © TUTTI I DIRITTI RISERVATI

L'opera, comprese tutte le sue parti, è tutelata dalla legge sui diritti d'autore. Sono vietate e sanzionate (se non espressamente autorizzate) la riproduzione in ogni modo e forma (comprese le fotocopie, la scansione, la memorizzazione elettronica) e la comunicazione (ivi inclusi a titolo esemplificativo ma non esaustivo: la distribuzione, l'adattamento, la traduzione e la rielaborazione, anche a mezzo di canali digitali interattivi e con qualsiasi modalità attualmente nota od in futuro sviluppata).

Le fotocopie ad uso personale del lettore possono essere effettuate nei limiti del 15% di ciascun volume dietro pagamento alla SIAE del compenso previsto dall'art. 68, commi 4 e 5, della legge 22 aprile 1941 n. 633.



*Un ringraziamento speciale ad "HT2", Community di
Manager, Professionisti, Imprenditori, Ricercatori,
Giovani Talenti con la vocazione di voler contribuire
allo sviluppo del nostro Paese attraverso
l'innovazione sostenibile.
Un cordiale benvenuto a tutti coloro che,
condividendo le nostre finalità, si iscriveranno al
nostro social (Facebook ht2, www.ht2.it)*

*Dedicato a mia figlia Alice Giulia
Questo libro la vede come co-autrice,
a partire dai primi brainstorming elaborati con lei,
durante gli anni di studio,
dapprima al Politecnico di Milano
poi alla DTU, Danmarks Tekniske Universitet di Copenhagen,
oggi alla NTU, Nanyang Technological University di Singapore,
dove si occupa di Quantum Computing ed Intelligenza Artificiale.
Alice Giulia ha fornito preziose indicazioni e spunti sempre più innovativi che
travalicano il modesto obiettivo di questo lavoro.
A lei il mio grazie più profondo.*

INDICE GENERALE

Introduzione	11
CAPITOLO 1	
QUANDO LE FORMICHE SI METTONO D'ACCORDO SPOSTANO L'ELEFANTE	
1.1 Dove siamo	22
1.1.1 <i>Finalmente sostenibilità</i>	
1.2 Il desiderio di cambiamento	24
1.2.1 <i>La crisi di valori nella società</i>	
1.2.2 <i>Il progresso nello spazio-tempo</i>	
1.2.3 <i>Il recupero della dimensione umana più profonda</i>	
1.2.4 <i>La collaborazione orizzontale p2p (peer-2-peer)</i>	
1.2.5 <i>Il fiasco della globalizzazione</i>	
1.2.6 <i>I segnali di una nuova società creativa e spirituale</i>	
1.2.7 <i>Il web 3.0</i>	
1.3 Un cenno ai sistemi distribuiti – Blockchain	37
1.3.1 <i>La decentralizzazione della Blockchain</i>	
1.4 La Blockchain semplificata	43
1.5 Una spiegazione semplificata dei modelli di consenso	51
1.6 Blockchain. Internet dei valori	56
1.6.1 <i>Controllo della Supply-Chain, riduzione delle emissioni</i>	
1.6.2 <i>Lotta alla corruzione</i>	
1.6.3 <i>I problemi umanitari e le migrazioni di massa</i>	
1.6.4 <i>Politica</i>	
1.7 L'approccio metodologico	61
CAPITOLO 2	
MODELLI DI CONSENSO	
2.1 Il problema generale del consenso.....	64
2.2 Regole dei sistemi distribuiti.....	68
2.3 Il Teorema CAP: <i>Consistency, Availability, Partition Tolerance</i>	73
2.4 Byzantine Fault Tolerance (BFT).....	78
2.4.1 <i>Il problema dei generali bizantini</i>	

2.5 Algoritmi di consenso classici o a voto esplicito.....	83
2.5.1 Paxos e Raft	
2.5.2 Practical BFT, Simplified BFT	
2.6 Algoritmi di consenso a voto implicito.....	90
2.6.1 Algoritmi di consenso Nakamoto	
2.7 Proof-of-Stake. Attacchi alla Blockchain. Nothing-at-stake	98
2.7.1 Nothing-at-stake	
2.8 PoS Chain-based e PoS BFT-based. Approfondimenti.....	106
2.9 Principi di Atomic Broadcast	108
2.10 Principi base del Protocollo di Gossip	111
2.11 Il protocollo Tendermint.....	115
2.12 Il protocollo Casper	121
2.13 Consenso federale (federated consensus).....	123
2.13.1 Consenso federale. Un caso di successo: Ripple	
CAPITOLO 3	
MANIPOLAZIONE DEL CONSENSO. TEORIA DEI GIOCHI	
3.1 Manipolazioni del comportamento. La Teoria dei Giochi	128
3.2 Teoria dei Giochi. Cenni	130
3.2.1 Teoria dei Giochi. Scelte indipendenti. Equilibrio di Nash	
3.2.2 Teoria dei Giochi. Scelte coordinate. Doppio equilibrio di Nash	
3.2.3 Teoria dei Giochi. Doppio equilibrio con influenza esterna	
CAPITOLO 4	
FONDAMENTI DELLA BLOCKCHAIN	
4.1 Fondamenti della Blockchain	136
4.1.1 I ledger. Cenni	
4.1.2 I componenti fondamentali della Blockchain	
4.1.3 Introduzione ai token	
4.1.4 Introduzione agli smart contract	
4.1.5 Il fork	
4.1.6 Ethereum. Cenni	
4.1.7 Blockchain e GDPR	
4.2 Breve storia della Blockchain	158

CAPITOLO 5	
CRITTOGRAFIA E BLOCKCHAIN	
5.1 La Crittografia	162
5.2 Hash Function.....	164
5.2.1 <i>Private e public Key. Firma digitale</i>	
5.2.2 <i>End-to-end encryption a chiave asimmetrica</i>	
5.2.3 <i>Merkle Tree</i>	
5.3 Zero-Knowledge-Proof (ZKP)	173
5.3.1 <i>Zero-Knowledge-Proof. La grotta di Alibaba</i>	
CAPITOLO 6	
MODELLI DI BLOCKCHAIN. PUBBLICHE, CONSORTIUM, PRIVATE.	
6.1 Dalle public Blockchain alle Enterprise Blockchain	178
6.2 Una visione più vicina all'azienda.....	180
6.3 Enterprise Blockchain.....	182
6.3.1 <i>Peculiarità delle Blockchain</i>	
6.4 Principali Blockchain a confronto.....	187.
6.4.1 <i>Ethereum</i>	
6.4.2 <i>Cosmos-Tendermint</i>	
6.4.3 <i>Cardano</i>	
6.4.4 <i>EOS</i>	
6.4.5 <i>Hyperledger</i>	
6.4.6 <i>Altri protocolli</i>	
6.5 Applicazioni della Blockchain al business	201
CAPITOLO 7	
FINANCING ED ANTIRICICLAGGIO	
7.1 ICO. Initial Coin Offering	210
7.1.1 <i>Ciclo di vita della ICO. Schema dei 7 passi</i>	
7.1.2 <i>Aree grigie delle ICO</i>	
7.1.3 <i>La filosofia ICO non tramonta</i>	
7.1.4 <i>Security Token Offering (STO)</i>	
7.2 Regolamentazione e Antiriciclaggio.....	219
7.2.1 <i>Anti-Money-Laundering (AML)</i>	
7.2.2 <i>Know-Your-Customer (KYC)</i>	
7.2.3 <i>Money Trasmitter Licence (MTL)</i>	

7.2.4	<i>Legislazioni e regolamentazione nel mondo</i>	
7.2.5	<i>Situazione italiana</i>	
CAPITOLO 8		
SCALABILITY, WEB3.0. METODOLOGIE		
8.1	Il problema della Scalability	226
8.2	Approccio intuitivo alla Scalability	229
8.3	Analisi di sensitività sulle variabili interne alla Blockchain	232
8.4	Suddivisione della Scalability in orizzontale e verticale.....	235
8.5	Scalability. Confronto Bitcoin vs Ethereum	237
8.6	Scalability verticale	240
8.6.1	<i>Scalability verticale di layer1. Variabile: Block Time</i>	
8.6.2	<i>Riduzione del Block Time. Riflessioni</i>	
8.6.3	<i>Scalability verticale di layer1. Variabile: Block Size</i>	
8.6.4	<i>Scalability verticale di layer1. Variabile: transazione</i>	
8.6.5	<i>Scalability verticale. Modello off-chain o layer2</i>	
8.6.6	<i>Scalability verticale di layer2. Private Payment Channel</i>	
8.6.7	<i>Scalability verticale di layer2. Lightning Network</i>	
8.7	Scalability orizzontale.....	256
8.7.1	<i>Scalability orizzontale di layer1. Sharding</i>	
8.7.2	<i>Scalability orizzontale di layer2. Side-chain</i>	
8.8	Scalability diagonale. Web3.0	259
CAPITOLO 9		
METODOLOGIE PER PROGETTARE LA PRIVACY		
9.1	Il problema della privacy e dell'anonimato	264.
9.2	Anonimato. Security vs decentralizzazione.....	265
9.3	Denonimyzation e pseudonimi	269
9.4	Mixing. Metodologie	271
9.4.1	<i>Mixing centralizzato</i>	
9.4.2	<i>Alcoin Exchange</i>	
9.4.3	<i>Mixing decentralizzato. Modello CoinJoin</i>	
9.4.4	<i>Mixing. Fair-Exchange</i>	
9.4.5	<i>Mixing Embedded nelle piattaforme</i>	
9.5	Cripto valute focalizzate sulla privacy e sull'anonimato.....	278
9.5.1	<i>Dash</i>	
9.5.2	<i>Monero</i>	

9.5.3 Zcash	
CAPITOLO 10	
VALORIZZAZIONE DELLA STRATEGIA PER LA BLOCKCHAIN	
10.1 La Blockchain fa sistema con le altre innovazione	286
10.1.1 AI, Artificial Intelligence	
10.1.2 IoT, Internet-of-Things	
10.1.3 AR/VR Augmented/Virtual Reality	
10.2 Sostenibilità e trasparenza premiano	290
10.3 La rivoluzione Blockchain non coglie i Big di sorpresa	292
10.3.1 Il cambiamento già in atto	
10.4 Cripto vs valuta fisica (fiat)	298
10.5 Il valore strategico della Blockchain	304.
10.5.1 Modello di adozione della Blockchain. A che punto siamo	
10.6 Strategia del Sistema Blockchain.....	308
10.7 Implementazione della strategia.....	311
10.7.1 Modello di valorizzazione della strategia	
10.7.2 Tradurre le idee in azioni	
10.7.3 Un esempio di disruption di business. La subscription	
CAPITOLO 11	
METODOLOGIE PER LO SVILUPPO DEGLI USE CASE	
11.1 Approccio metodologico per lo sviluppo degli use case	322
11.1.1 Due passi propedeutici: Single Customer View e Innovation Hub	
11.2 Metodologia Ten Step Plan	329
11.2.1 Ten-step-Plan	
11.2.2 Finalizzazione degli use case	
11.2.3 25 esempi di use case nel CPG-Retail	
CAPITOLO 12	
METODOLOGIE DI PROGETTAZIONE DELLA BLOCKCHAIN	
12.1 Approccio alla Progettazione & Selezione della Blockchain	34
2	
12.1.1 Algoritmo di consenso: il pivot della progettazione	
12.1.2 Vincoli e limiti attuali alla progettazione	
12.2 Metodologia. Progettazione e Selezione.....	347

12.2.1	Metodologia. Sharp Cut: go, no go	
12.2.2	Modello dei 7 componenti chiave della Blockchain	
12.2.3	Modello di Engagement	
12.3	Checklist per la verifica di massima della Blockchain	35
8		
12.4	Tokenization. Standard ERC-20, ERC-721	36
3.		
12.4.1	GAS per far girare lo smart-contract con il motore EVM	
12.4.2	ERC-20 e ERC-721	
12.5	Standard Blockchain. Stato dell'arte	376
CAPITOLO 13		
ALTERNATIVE ALLA BLOCKCHAIN. UNO SGUARDO AL FUTURO		
13.1	Non solo Blockchain	378
13.2	Ledger distribuiti di nuova generazione	382
13.2.1	HASHGRAPH	
13.2.2	DAG	
13.2.3	HOLOCHAIN	
13.2.4	RADIX (TEMPO)	
CAPITOLO 14		
CHANGE MANAGEMENT NEI SISTEMI DECENTRALIZZATI		
14.1	Change Management nei sistemi decentralizzati	388
14.2	La piattaforma di Change Management	391
14.2.1	Da agenti ad ispiratori del cambiamento	
14.2.2	I driver del cambiamento	
APPENDICE 1		
	AZIONI DI INNOVAZIONE. CREATIVITA', SOSTENIBILITA', DEMOCRAZIA	399
APPENDICE 2		
	MAPPA ECOSISTEMI DEI PROGETTI BLOCKCHAIN E DELL'AREA MARKETING	417

Bibliografia	426
--------------------	-----