Roberto Garavaglia

Tutto su BLOCKCHAIN

Capire la tecnologia e le nuove opportunità

HOEPLI

Tutto su Blockchain

Roberto Garavaglia

Tutto su Blockchain

Capire la tecnologia e le nuove opportunità

EDITORE ULRICO HOEPLI MILANO

Copyright © Ulrico Hoepli Editore S.p.A. 2018
via Hoepli 5, 20121 Milano (Italy)
tel. +39 02 864871 – fax +39 02 8052886
e-mail hoepli@hoepli.it

www.hoepli.it

Seguici su Twitter: @Hoepli_1870

Tutti i diritti sono riservati a norma di legge
e a norma delle convenzioni internazionali

ISBN EBOOK 978-88-203-8498-2

Progetto e realizzazione editoriale:
Maurizio Vedovati – Servizi editoriali
(info@iltrio.it)

Copertina:
Sara Taglialegne

Realizzazione digitale:
Promedia, Torino

A Mela,
per la sua capacità di comprendere
ascoltando
e di ascoltare comprendendo.

INDICE

4 Le regole del consenso e della fiducia in una blockchain

Modello di governo centralizzato

Modello del governo centralizzato e dei controlli distribuiti

Modello del governo condiviso e del controllo distribuito

5 Gli scambi di valore nei periodi del

governo centralizzato

- Il deposito di Alice nel periodo del governo centralizzato
- Il trasferimento degli asset di Alice verso Bob nel periodo del governo centralizzato
- Il lavoro di validazione di Trent
  - Un modo alternativo per controllare la reale disponibilità di Welthy non spesi
- Gli scambi di valore nel periodo del governo centralizzato e dei controlli

distribuito

- Cosa significa verificare una transazione e validare una pagina di transazioni verificate
- La validazione delle pagine contabili di un registro distribuito
- La prova di lavoro per la validazione delle pagine di un registro distribuito
- Il problema del “Double Spending”
  - La ricompensa dei validatori delle pagine di un registro distribuito
- Le transazioni sul registro

distribuito

Cosa potrebbe accadere nel caso di “Double Spending”

Gli incentivi per i validatori delle transazioni su un registro distribuito

7 Che cosa sono gli asset nativi

Il legame dell’asset nativo con il mondo degli scambi in un’economia reale

8 Centralized Ledger vs Distributed Ledger

L’analisi SWOT per la fase 1

(Centralized Ledger)

I punti di forza nella fase 1 (modello del governo centralizzato)

I punti di debolezza nella fase 1 (periodo del governo centralizzato)

Le opportunità nella fase 1 (periodo del governo centralizzato)

I rischi nella fase 1 (periodo del governo centralizzato)

L'analisi SWOT per la fase 2 (Shared Decentralized Ledger)

I punti di forza nella fase 2 (modello del governo

centralizzato e dei controlli distribuiti)

I punti di debolezza nella fase 2 (modello del governo centralizzato e dei controlli distribuiti)

Le opportunità nella fase 2 (modello del governo centralizzato e dei controlli distribuiti)

I rischi nella fase 2 modello del governo centralizzato e dei controlli distribuiti)

L'analisi SWOT per la fase 3 (Shared Distributed Ledger)

I punti di forza nella fase 3 (modello del governo

Parte II. All'interno della

Blockchain

9 La Blockchain con la “B” maiuscola

- Che cos’è una Blockchain
- L’utilità della Blockchain
- Non confondiamo i Bitcoin con la Blockchain, ma contemperiamoli!
- Alcune definizioni per descrivere la Blockchain
  - Criptoasset
  - BTC
  - Nodo
  - Transazione

Blocco

Ledger

Hash (o funzione di Hash)

Target

Difficoltà

Miner (o minatore)

Mining

PoW, Proof-of-Work (o prova di lavoro)

Nonce

Reward (o ricompensa)

Mance (o commissioni)

Protocollo

Network

Wallet

Firma digitale

- Blockchain
  - Gli Output e gli Input di una transazione
- L'invio di una transazione ai nodi del network
- La verifica di una transazione sulla Blockchain
- La creazione di un blocco sulla Blockchain
- La validazione di un blocco sulla Blockchain
  - L'attività di mining
  - Come evitare il "Double Spending" sulla Blockchain
- La propagazione dei blocchi sulla Blockchain

15 Le principali blockchain

Ethereum

Che cos'è Ethereum

Ether e Gas: la moneta di scambio e il "carburante" di Ethereum

Ethereum Virtual Machine EVM: il "motore" di Ethereum

I linguaggi di programmazione impiegati su Ethereum

La profonda frattura venutasi a creare sul concetto di base di una

16 Nella galassia delle DLT

Computing

18 Nel regno del Distributed Computing

Distributed Contract

Il ciclo di vita di una transazione governata da uno Smart Contract

Gli Smart Contract di Ethereum

19 DAO – Decentralized Autonomous Organization

Parte V. Gli ambiti applicativi cross-industry

20 Oltre alle criptovalute c’è di più

21 La blockchain in contesti cross-industry

Caratteristiche e benefici

I principali driver che identificano i migliori casi d'uso

22 Settori di applicazione

Agrifood

Assicurazioni

Banking

Digital marketing

Parte VI. Scenari e strategie

23 Scenari

- Che cos’è il Lightning Network
- Che cos’è IOTA
- I maggiori limiti delle blockchain
  - Centralizzazione del controllo
  - Crittografia quasi obsoleta
  - Gestione delle Fork
  - Separazione dei ruoli tra i partecipanti a una blockchain
  - Limiti di scalabilità
  - Consumo energetico
- Guardiamo più in là…

Il cambiamento dovrebbe
essere un amico.
Dovrebbe accadere perché
programmato,
non a seguito di un incidente.

Philip Bayard Crosby

Prefazione

Molto si è detto dei rischi legati all'impiego delle criptovalute, di cui i Bitcoin sono l'espressione più nota. Molto meno si è discusso sui possibili benefici correlati all'uso della tecnologia che vi sottende. L'obiettivo di questo libro non è valutare le utilità di una criptovaluta, bensì evidenziare e analizzare le opportunità derivanti dall'applicazione accorta e lungimirante della Blockchain, ossia la tecnologia che supporta le transazioni in valuta virtuale emesse in modo decentralizzato. Le Distributed Ledger Technologies (DLT), i protocolli di consenso

distribuito e l'esecuzione autonoma e decentrata degli Smart Contract, propongono nuovi paradigmi che rivoluzionano fortemente il sistema economico, modificando alla base i concetti di transazione, proprietà e fiducia. Capire il significato di termini come "criptoasset" e "cryptoeconomy" nella loro accezione essenziale permette di comprendere quali possano essere gli ambiti di applicazione di queste tecnologie che più di altri avranno possibilità di essere apprezzati nei prossimi anni. Ho scritto questo libro per consentire a chiunque voglia investire nel cambiamento portato dalla Blockchain di orientarsi verso direttrici di sviluppo a maggior "grado di

resilienza", esercitando un pensiero laterale affrancato dalle logiche tradizionali. Se a fine lettura sarete in grado di discernere i Bitcoin dalla Blockchain, comprendendo che ogni grande invenzione dell'uomo può essere utile e dannosa, ma ciò dipende unicamente dall'uso che si vuole farne, se sarete in grado di obiettare a quelli che dicono "i Bitcoin no, ma la blockchain sì" opponendo il concetto razionale al preconcetto emotivo, allora sarò riuscito (forse anche solo in parte) a tracciare un solco nel quale seminare granelli di un cambiamento concreto (non solo annunciato) e i frutti che ne verranno saranno alla portata di tutti.

Roberto Garavaglia

L’autore

Roberto Garavaglia è un consulente strategico nel settore dei sistemi di pagamento digitali, da oltre venticinque anni specializzato nell’ideazione di nuovi modelli di business e prodotti innovativi. Nel 2014 è fra i primi in Italia a occuparsi di progetti blockchain in ambito finance. Accanto agli impegni di strategic advisor, svolge attività di divulgazione scientifica e di docenza presso imprese e università. Dal 2008 collabora con il Politecnico di Milano – Osservatori Digital Innovation, contribuendo con la propria esperienza all’analisi delle strategie in ambito New

Digital Payments e tenendo corsi su Blockchain e sugli scenari di mercato che possono orientarne uno sviluppo cross-industry. Ha al suo attivo innumerevoli pubblicazioni scientifiche sviluppate nell'ambito degli Osservatori del Politecnico di Milano, su temi che concernono l'innovazione e la regolamentazione dei sistemi di pagamento innovativi. Nel 2007 idea il concept "Pagamenti 2.0", declinazione di un servizio di pagamenti digitali lungo gli scenari socioeconomici emergenti delle architetture partecipative, e definisce il ruolo di un nuovo soggetto economico: il "Payment Services Consumer".

Nel marzo del 2008 progetta e avvia il blog www.closetopay.com, la prima iniziativa tesa a diffondere cultura nei settori e-Payment e m-Payment, con l'obiettivo di contribuire a colmare il gap culturale fra utenti e fornitori di servizi di pagamento. Nel 2013 avvia il portale PagamentiDigitali.it, di cui è coordinatore editoriale. Nel 2017 contribuisce al lancio del nuovo progetto editoriale Blockchain4Innovation del gruppo Digital360. Nel 2016 è owner e scientific advisor del tavolo di lavoro "Pagamenti Digitali" nell'ambito dell'iniziativa "Cantieri della PA Digitale" promossa da ForumPA; il

tavolo, partecipato da Regioni, enti locali, associazioni di categoria e istituzioni, produrrà il documento di advocacy "Il digitale che entra nei sistemi di pagamento alla PA", che offrirà spunti importanti per la legiferazione del nuovo CAD (Codice di Amministrazione Digitale). Membro AITI (Associazione Italiana Tesorieri d'Impresa) dal 2009 al 2016, si è occupato in Commissione Pagamenti di Cards & Innovative Payments. Dal 2009 al 2016 partecipa attivamente come EACT (European Association for Corporate Tresaures) ai gruppi di lavoro europei in materia di innovazione dei sistemi di pagamento: EPC CSG – Card Stakeholders Group, PSMEG –

Payment Systems Market Expert Group.

Introduzione

Comprendere che cosa sia la Blockchain è probabilmente più semplice di quanto si creda. Capire perché la Blockchain rappresenti una delle più straordinarie tecnologie innovative degli ultimi anni è forse più complesso. Avviciniamoci quindi con serenità d'animo e mente aperta a questa affascinante materia, con l'obiettivo di percorrere, passo dopo passo, la strada avviata da Satoshi Nakamoto, colui cui si attribuisce la paternità putativa dei Bitcoin (uno pseudonimo dietro al quale, ancora oggi, non si è scoperto chi vi sia), che per primo ha ipotizzato come un pensiero

economico tradizionale potesse declinarsi, tramite l'impiego di più tecniche digitali già presenti da molti anni (crittografia, protocolli di trasmissione, marcatura temporale), dando origine a un nuovo concetto di "criptoeconomy". Il significato cui il misterioso fautore della più famosa criptovaluta, nonché ideatore della Blockchain, voleva riferirsi è, con buona probabilità, quello volto a intendere l'economia nell'accezione più antica del termine, ossia quella che ne interpreta l'essenza come scienza della soddisfazione e del fabbisogno attraverso lo scambio.

Satoshi, di per sé, come tutti gli

inventori più illuminati, non ha creato nulla dal nulla, bensì ha strutturato in forma digitale un sistema che consente di riproporre qualcosa che già esisteva, ma che poteva realizzarsi solo nel mondo materiale e delle convenzioni: il trasferimento di valore.

Nel mondo tradizionale esistono gli scambi di informazioni e il trasferimento di beni fisici o competenze, ossia valori che assumono tale significato in quanto scarsi. L'avvento di Internet ha consentito a una pluralità più ampia di accedere e distribuire le informazioni. Grazie alla tecnologia ognuno può intervenire sul dato stesso replicandolo (anche all'infinito), modificandolo e

rimettendolo in circolo. Il bene fisico, in quanto scarso, possiede un valore che, sino all'avvento della Blockchain, non era pensabile poter trasferire al pari delle informazioni.

Se un fotografo distribuisce il frutto del proprio lavoro via Internet, sa che dovrà fare i conti con – almeno – due aspetti caratterizzanti il sistema che ha scelto di impiegare per negoziare i propri prodotti (fotografie, filmati): la replicabilità e, al suo opposto, la censura.

In tal senso, laddove il fotografo non prendesse accorgimenti per tutelare i propri diritti, ognuno potrebbe

inflazionare la sua produzione (creando infinite copie delle sue opere).

La tutela dei propri diritti implica necessariamente che il fotografo abbia fiducia in una (o più) parti della filiera produttiva e distributiva; per esempio il provider di rete, il gestore del sistema di pagamento, le autorità che sovrintendono e regolano i diritti dell'autore e di sfruttamento dell'opera stessa o le istituzioni pubbliche che legiferano e governano in materia di liberi scambi e così via.

Per poter eseguire un trasferimento di valore via Internet, dunque, era necessario trovare un metodo che

rendesse molto difficile vanificare l'immutabilità delle transazioni, che fosse il più possibile immune da un attacco esterno, volto ad alterarne le proprietà, e che potesse garantire tutto ciò anche in assenza di fiducia.

Blockchain è questo: un sistema matematico che ripropone nel digitale il concetto di scarsità, consentendo lo scambio di asset immune al rischio di replica, trasparente e tracciabile.

Su queste basi alcuni ritengono che la Blockchain sia la nuova generazione di Internet, o meglio ancora la "Nuova Internet". Noi riteniamo che la Blockchain possa rappresentare la

Internet del Valore e, su tale assunto, vogliamo condurvi con questo libro nel merito di un'esplorazione che, ci auguriamo, possa permettere a ognuno di comprendere ciò che si può fare e ciò che ha poco senso realizzare, volendo cogliere i reali ed effettivi benefici derivanti dall'uso di questa tecnologia.

Buona lettura.

Cronistoria della Blockchain

All'inizio fu un white paper

- 31 ottobre 2008: Satoshi Nakamoto pubblica il "Bitcoin design paper", un white paper nel quale spiega la sua idea di moneta virtuale Peer-to-Peer risolvendo il problema del Double Spending.
- 3 gennaio 2009: nasce il

"Genesis block" alle 18:15:05 GMT.

Poi, dopo qualche problema non del tutto trascurabile che connoterà negativamente il significato di Blockchain ancorandolo al Bitcoin, si arriva a un primo interesse dei regolatori, ancora però concentrato solo sulla valuta virtuale.

- 4 luglio 2014: l'EBA (Autorità Bancaria Europea) pubblica il suo paper "Opinion on 'virtual currencies'" con cui raccomanda ai legislatori europei di applicare le leggi antiriciclaggio e di contrasto

al finanziamento del terrorismo ai mercati di valute virtuali.

Si arriva dunque al 2015 e, nell'arco di un anno, le tematiche Blockchain e Distributed Ledger vivranno un vero e proprio hype di comunicazione, ottenendo le copertine di importanti riviste internazionali e venendo annoverate tra i trend tecnologici più interessanti a livello mondiale.

È anche la prima volta che si inizia a parlare non solo di Bitcoin; il mondo sembra accorgersi che esiste qualcosa "sotto" alla criptovaluta più popolare che merita un'attenzione diversa: la Blockchain.

Nel frattempo, però, era successo qualcosa:

- Dicembre 2013: parte lo sviluppo di Ethereum e agli inizi di febbraio 2014 vengono rilasciate le prime versioni.
- Primi mesi del 2014: Ripple recluta due banche statunitensi, CBW Bank of Topeka e Cross River Bank of Teaneck. Sono le prime a partecipare al sistema di pagamenti che consentirebbe pagamenti istantanei e gratuiti transfrontalieri sulla

Rete.

Tra il 2015 e il 2016 è tutto un tripudio:

- Ottobre/novembre 2015: prima pagina dell'*Economist* dal titolo: "The trust machine – How the technology behind bitcoin could change the world".
- Nel corso del 2015 nasce il consorzio R3, che si pone l'obiettivo di definire i protocolli standard nell'utilizzo della Blockchain nel settore bancario.

- Fine 2015/inizi 2016: la Linux Foundation annuncia l'inizio del suo progetto "Hyperledger" per la creazione di una struttura di Distributed Ledger open source.
- Metà 2016: UBS, Deutsche Bank, Santander e Bank of New York Mellon creano la "utility settlement coin", che mira a permettere il pagamento per asset come bond e titoli da parte delle istituzioni finanziarie, senza attendere il trasferimento di denaro tradizionale.

- Fine 2016: R3 rilascia il codice per la sua tecnologia di Distributed Ledger: Corda.
- Fine 2016: SWIFT annuncia il suo primo proof-of-concept su blockchain e si impegna a diventare un punto di riferimento per la comunità finanziaria nell'applicazione della tecnologia.

E anche i regolatori non stanno a guardare:

- Inizi del 2015: il governo dell'Honduras insieme a

Factom inizia lo sviluppo di un registro di titoli di proprietà terriere basato sulla blockchain.

- Seconda metà del 2015: il governo Estone annuncia l'inizio di una partnership con Bitnation per offrire un servizio di notarizzazione pubblico basato su blockchain.

Seconda metà del 2016: il governo del Regno Unito sperimenta la blockchain per effettuare pagamenti nel Welfare.

Il 2017 è l'anno in cui anche in Italia qualcosa si muove:

- Intesa Sanpaolo e UniCredit partecipano alla sperimentazione GPI (Global Payment Innovation) di SWIFT.
- SIA, operatore specializzato in servizi tecnologici dedicati alle Istituzioni Finanziarie, Banche Centrali, Imprese e Pubbliche Amministrazioni, annuncia la sua piattaforma blockchain: SIAChain.
- ABI Lab annuncia la fase operativa della sperimentazione di un progetto, che coinvolge 12

banche italiane, basato su Distributed Ledger Technology applicata al processo di spunta interbancaria.

PARTE I

I FONDAMENTALI

In un'economia di conoscenza, un buon affare
è una comunità con uno scopo, non una proprietà.

Charles Handy

1

Per iniziare

Nel mondo materiale delle cose, degli uomini e della loro storia, vi è un'attività i cui principi risalgono probabilmente alla nascita delle prime forme di organizzazione sociale: lo scambio di beni e servizi che hanno un valore.

Per rendere più semplice la comprensione di cosa sia una

blockchain, nel corso dei capitoli racconteremo di una immaginaria società di individui che chiameremo Welthyland, nella quale esiste un mercato degli scambi cui si deve avere accesso per poter inviare e ricevere beni. La metafora faciliterà, in ogni istante, la comprensione dei modelli (centralizzati, decentralizzati, distribuiti) e dei processi che permettono alle diverse blockchain di distinguersi.

Iniziamo dunque dai fondamentali.

Blockchain e Bitcoin: attenzione

a come sono scritte le iniziali

“Blockchain” con l’iniziale maiuscola indica la tecnologia che supporta i Bitcoin, mentre “blockchain” con l’iniziale minuscola sta per l’architettura tecnologica posta alla base di altri sistemi dove il criptoasset non è necessariamente il Bitcoin. Convenzionalmente, il termine “Bitcoin” è utilizzato con l’iniziale maiuscola quando ci si vuole riferire alla tecnologia e al protocollo di rete (ossia alla Blockchain), mentre l’iniziale minuscola (“bitcoin”) è impiegata se ci si vuole riferire alla criptovaluta in sé.

2

Il valore degli scambi e gli scambi di valore

A Welthyland ognuno può scambiarsi qualcosa cui la comunità ha attribuito un valore. Per definizione, chiameremo questo “qualcosa” Welthy e le transazioni di valore saranno transazioni

di Welthy.

Prima di addentrarci nel nostro racconto, capiamo che cosa sono (o a che cosa potrebbero essere assimilati, non senza cedere a qualche compromesso di significato, nell'economia reale) i Welthy.

Definizione di moneta

In economia il termine "moneta" definisce l'insieme dei valori che vengono regolarmente adottati da ogni individuo appartenente a una società per negoziare beni e servizi.

La moneta svolge tre funzioni:

- mezzo di scambio;

- unità di conto;
- riserva di valore.

Intesa come mezzo di scambio, la moneta è impiegata come sistema per intermediare la negoziazione di merci (evitando il baratto), rispondendo con ciò all'esigenza di conciliare le volontà di due parti coinvolte in una transazione di pagamento.

Nell'accezione di unità di conto, la moneta serve per la computazione del valore e del costo di un bene, di un servizio, di un credito o di un debito. Come riserva di valore consente a ognuno che ne dispone di trasferire nel tempo (dal presente al futuro) il potere di acquisto.

Storicamente è difficile far risalire a una precisa data l'inizio della moneta. Sembra che già nel 2200 a.C. avvenissero scambi di merce contro moneta. Il suo significato era, a questo stadio primordiale, inteso come commodity, laddove intrinsecamente connesso al valore di un oggetto (per esempio bestiame o, più tardi, argento e oro).

Intorno al XVIII secolo d.C. inizia a circolare una moneta consistente in oggetti unicamente rappresentativi del valore sottostante; si parla in questo caso di "Commodity-backed money". Con questo significato, la moneta diventa portabile, quindi più

agevolmente scambiabile ma anche altrettanto facilmente accumulabile.

Nelle moderne economie, la moneta acquista un nuovo significato di "moneta *fiat*" e, privata di qualsiasi valore intrinseco, diviene a corso legale (si parla dunque di valuta legale). Viene considerata moneta in forza di un atto legislativo e il suo valore è fissato da un'autorità, ossia lo Stato, che si fa garante della sua stabilità e la riconosce come mezzo di pagamento. La negoziazione di merci avviene tramite lo scambio di una valuta legale, poiché ciascun soggetto (pagatore e beneficiario) ha fiducia nell'autorità centrale che la emette[1]. La fiducia è un

elemento essenziale della "moneta *fiat*". Impiegata come mezzo di pagamento ha valore liberatorio, ossia ha il potere di estinguere le obbligazioni pecuniarie tra pagatore e beneficiario.

Definizione di asset

Sulla base di quanto abbiamo sin qui ricordato è corretto dire che i nostri Welthy siano una moneta? Potrebbero forse essere meglio descritti come asset? Ma che cos'è un asset?

In senso molto ampio, ogni entità materiale o immateriale suscettibile di valutazione economica, per un certo soggetto, è considerata un asset. Sempre

più spesso, però, i diritti connessi all'utilizzo e allo sfruttamento delle attività, materiali o immateriali che siano, si concentrano in titoli finanziari rappresentativi dei diritti stessi (per esempio azioni o obbligazioni).

Se per semplicità assumiamo che un asset possa essere un oggetto (materiale o immateriale, oppure fisico o digitale o, ancor meglio, un "neobene"[2]), che cosa – ancor prima di chi – conferisce valore a un oggetto? Il suo essere capace di conseguire un fine o la convinzione, di un soggetto, che l'oggetto sia funzionale al suo perseguimento.

Facciamo alcuni esempi. L'acqua possiede un valore maggiore nei Paesi

in cui vi è siccità e minore in quelli dove esistono impianti di stoccaggio e conduzione; una pianta di gerani varrà di più in quei luoghi dove vi sono molte zanzare, perché si è convinti che il geranio abbia il potere di allontanare quegli insetti. Una banconota rappresentativa di una moneta ha valore solo se vi è un mercato. Ciascuno di questi oggetti esiste "per sé" e non potrebbe avere un valore se non mediante l'attribuzione, autonoma e arbitraria, a carico di qualcuno che ne vede l'utilità come mezzi per l'ottenimento (o anche solo la facilitazione) di uno scopo; una valutazione che diremo, dunque,

soggettiva[3].

Il nostro Welthy, dunque, è assimilabile al concetto di asset (nella sua più ampia accezione) laddove gli individui che abitano a Welthyland ne attribuiscono un valore specifico per uno scopo, mentre sarebbe ascrivibile nella categoria delle valute (ovviamente n o n *fiat*) qualora vi fosse un'imposizione da parte del governo della nostra comunità immaginaria che lo rendesse, a corso forzoso, mezzo di pagamento.

Definizione di criptoasset

Per spiegare nel modo il più possibile "laico" che cosa sia la blockchain, dobbiamo assumere che a Welthyland vi sia un'economia basata unicamente sugli scambi di valore e che i Welthy, intesi come asset, siano rappresentazioni digitali di valore[4] che definiremo "criptoasset".

I trasferimenti di Welthy avvengono tra i membri della comunità e hanno sempre il significato di trasferimento delle disponibilità che ogni individuo vanta nel rispetto della comunità stessa. La disponibilità di Welthy e tutti gli scambi di tale diritto a disporne sono acclarati da qualcuno che gode della fiducia di ogni membro.

La custodia dei criptoasset

È importante osservare come, volutamente, non ci si preoccupa di mantenere l'oggetto rappresentato da Welthy – nel proprio valore – al riparo o custodito in cassaforte. L'appartenenza dell'oggetto all'effettivo titolare, così come la sua custodia, sono a carico del cittadino che dimostra di possederlo sulla base di un titolo (potremmo chiamarlo titolo di legittimazione) di cui si tiene traccia degli scambi.

La custodia di questo titolo è invece molto importante e ciascun cittadino è responsabile dei sistemi di sicurezza che

impiega per garantirla[5].

Cosa deve essere custodito di un criptoasset

Come vedremo nei successivi paragrafi, quando parleremo di Welthyland nella sua fase 3, ossia quella in cui vige un modello di governo condiviso e controllo distribuito a garanzia della validità di ciò che viene scambiato fra individui[6], la sicurezza legata a un criptoasset risiede nella possibilità che possa riconoscersene la proprietà in

modo univoco all'interno della comunità in cui viene scambiato. La dimostrazione dell'appartenenza di un criptoasset a qualcuno avviene mediante l'apposizione di una firma digitale[7] da parte di quel "qualcuno" che ne vanta la proprietà. Tale firma accompagnerà ogni transazione e permetterà, in tal modo, di consentire a chiunque di verificare che il criptoasset scambiato sia effettivamente appartenente al legittimo proprietario (o "cedente", stante l'atto di trasferimento della proprietà[8] del criptoasset, che avviene mediante una transazione tra pagatore e beneficiario). A scambio avvenuto, il ricevente (o cessionario) potrà controllare l'effettiva originaria

appartenenza del criptoasset[9] e disporne solo se in possesso di un codice segreto che gli permetterà di usarlo, a propria volta, per successivi scambi[10].

Dove deve essere custodito un criptoasset

Il codice segreto, mediante cui il destinatario di un trasferimento in Welthy può disporre dei criptoasset, dovrà essere custodito in un luogo protetto e sicuro[11]; l'eventuale perdita o furto è tale da permettere a chiunque ne

entrasse in possesso di dimostrare la proprietà del criptoasset.

È importante osservare, dunque, che all'interno di questo luogo sicuro non sono riposti i Welthy, bensì unicamente i riferimenti ai medesimi, accessibili (o, meglio, disponibili) solo tramite l'uso del codice segreto di cui sopra.

Chi scambia i valori

Prima di raccontare come gli abitanti di Welthyland si scambiano le disponibilità dei loro Welthy, facciamo la conoscenza di alcuni di loro: Alice, Bob, Charlie, Dan, Erin, Trent, Mallory e Grace (Figura 2.1); questi ultimi tre,

come vedremo, in realtà non sono dei veri e propri singoli individui, bensì delle “entità” che possono essere anche collettive. Per tale motivo sono state illustrate in Figura 2.1 con una marcatura diversa, figurativamente attinente le loro caratteristiche peculiari.

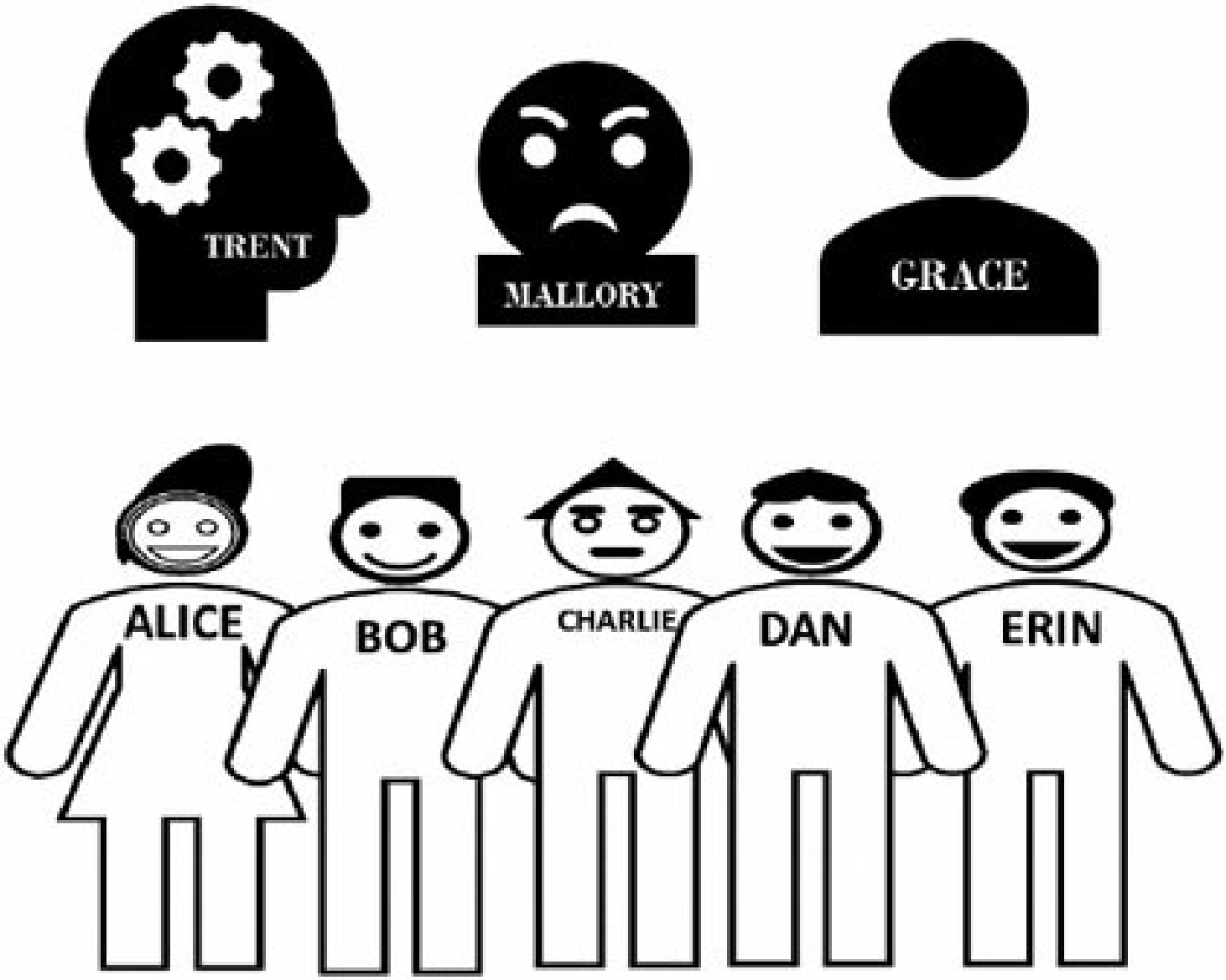

Figura 2.1 – I membri della comunità di Welthyland.

Ciascun personaggio ha una propria personalità che ne caratterizza il ruolo (o la funzione) nella società immaginaria

in cui abbiamo pensato di ambientare il racconto.

Alice e Bob sono due conoscenti (non necessariamente amici) che vogliono scambiarsi Welthy. Per il fine che il nostro racconto si prefigge, non è rilevante sapere perché Alice voglia inviare a Bob una parte dei suoi Welthy, ma è importante sapere che ne dispone di una quantità sufficiente per avviare lo scambio e, altro aspetto che va chiarito sin da subito, il trasferimento che avrà luogo sarà inteso come una sorta di trasferimento di proprietà dei beni, il cui valore è rappresentato dai Welthy. In altre parole, Bob riceverà da Alice una sorta di diritto a disporre dei "Welthy-asset" che, prima dello scambio, erano

nella disponibilità di Alice.

Charlie, Dan ed Erin sono altri tre personaggi che possono, a loro volta, ricevere o inviare Welthy a Bob ed Alice, ma anche scambiarseli tra di loro.

Per poter informare la controparte beneficiaria del trasferimento, ognuno usa degli strumenti di comunicazione che permettono di notificare sia la volontà di eseguire uno scambio sia l'avvenuto scambio[12].

Il vecchio Trent e il suo mastrino

Trent rappresenta il vecchio saggio di

Welthyland; il garante *super partes* di cui tutta la comunità si fida, il custode della verità. A Trent tutti si rivolgono per avere garanzia della bontà dei loro scambi di valore.

Trent è colui che annota il dare e avere di tutti i cittadini di Welthyland sul proprio libro mastro, di cui garantisce il mantenimento integro e inalterato (uno dei suoi compiti principali, unitamente a quello di "notaio" delle transazioni). È lui che tiene traccia, in modo puntuale e meticoloso, di tutti gli scambi di Welthy avvenuti sin dalla costituzione della comunità. Trent custodisce le chiavi della cassaforte in cui viene riposto il libro delle transazioni.

Sul mastrino di Trent, la traccia immutabile di qualsiasi movimento di valori tra gli abitanti di Welthyland, si attesta la proprietà, in ogni istante, dei Welthy in circolazione. Ciascun membro della comunità sa, dunque, che potrà disporre di un patrimonio il cui saldo è stato movimentato, nel tempo, dalle transazioni scritte sul documento aggiornato da Trent.

Il libro mastro è firmato da Trent o, meglio, ciascuna pagina[13] del libro viene firmata da Trent che, per efficientare il processo di contabilità, riporta alla fine di ogni foglio un saldo disponibile complessivo di Welthy riferito ai singoli abitanti di

Welthyland[14]. Trent è autonomo anche nella decisione di chiudere il foglio contabile, ossia può decidere a proprio piacimento dopo ogni quante transazioni in Welthy viene chiusa la pagina e calcolato il saldo disponibile. Oppure può decidere un intervallo di tempo prefissato entro cui deve essere chiusa la pagina contabile, a prescindere dal numero di transazioni registrate.

Trent, tuttavia, non può decidere autonomamente quali debbano essere i calcoli da effettuare per validare il processo contabile a fine pagina. Il saldo delle transazioni, infatti, inteso solo come una banale computazione del dare e avere complessivo di tutti i conti

in Welthy riportato a fine pagina, potrebbe non bastare per validare l'insieme di transazioni compiute nell'intervallo di tempo designato. Potrebbe rendersi necessario, per esempio, che unitamente al calcolo algebrico dei saldi movimentati, Trent produca una prova[15] che testimoni la sua notevole capacità computazionale (una delle ragioni per cui tutti si fidano di Trent), da trascrivere accanto a ogni saldo di pagina.

La fiducia in Trent

Trent conosce tutti, tutti conoscono Trent e l'intera comunità vi fa completo

affidamento; egli ha dunque un enorme potere che, al tempo stesso, è anche la sua debolezza: è solo ed unico.

Trent può improvvisamente ammalarsi e degradare le proprie prestazioni al servizio della collettività. Per evitare il verificarsi di tali conseguenze, potrebbe decidere di avvalersi di alcuni collaboratori fidati, ai quali, comunque, non assegnerà mai alcun poter decisionale. Trent, in quanto statutariamente solo, è esposto al rischio di vaneggiamenti e, nei casi più gravi, può impazzire e nuocere gravemente alla società.

---

1. Per questo motivo la "moneta *fiat*" è anche

chiamata valuta fiduciaria.

2. "I neobeni si caratterizzano e specializzano per alcune proprietà che li distinguono dai beni fisici, tra cui vale rilevare: la possibilità di essere diffusi, scambiati e acquisiti indipendentemente dalla forma tecnica su cui sono registrati, la riproducibilità, la possibilità di essere fruiti non solo senza esaurimento, ma, al contrario, incrementando e arricchendo la loro efficacia, per il tramite di un uso reiterato. Tali caratteristiche consentono ai neobeni una valorizzazione economica differente, dipesa anche dall'immaterialità e dall'azzeramento del 'costo del venduto'". Garavaglia R., "Un sistema di incasso-pagamento per i neobeni", *Bancamatica*, luglio/agosto 2010.

3. Seguendo questa logica potremmo arrivare a dire che anche questo libro che state leggendo costituisce un asset che vi faciliterà il

conseguimento di uno scopo: la comprensione della blockchain.

4. Successivamente, spiegheremo come sia possibile "legare" al Welthy un asset anche non digitale, per comprendere quali possano essere gli usi della blockchain anche al di fuori del perimetro "funzionalmente soggettivo" conferito dai cittadini di Welthyland.

5. Nelle blockchain si utilizzano dei sistemi di sicurezza basati su una coppia di chiavi pubbliche e private.

6. Questo è il caso della Blockchain dei Bitcoin, per esempio, e, più in generale, di tutte le blockchain pubbliche dove l'accesso al registro distribuito avviene senza alcuna predeterminazione di nessuna autorità centrale (si parla di "Permissionless Ledger").

7. La firma avviene mediante l'impiego della chiave privata del cedente (o mittente); per un maggior dettaglio si veda il paragrafo "Alcune

definizioni per descrivere la Blockchain".

8. Più correttamente si dovrebbe parlare di negozio giuridico.

9. Ciò avviene tramite l'uso della chiave pubblica del cedente (o mittente) che è nota a tutti proprio in quanto pubblica; per un maggior dettaglio si veda il paragrafo "Alcune definizioni per descrivere la Blockchain".

10. Ciò avviene tramite la chiave privata del destinatario che sarà impiegata, a propria volta, per firmare le transazioni che il medesimo vorrà eseguire successivamente.

11. Nelle blockchain questo luogo è chiamato "wallet".

12. Nella Blockchain questi strumenti vengono chiamati "nodi" e permettono a ciascun individuo dotato del proprio wallet di trasferire le disponibilità non spese di asset.

13. Le "pagine" del libro mastro nella

Blockchain sono chiamate "blocchi".

14. In realtà sulla Blockchain non esiste un concetto di "saldo" e neppure di "conto"; l'equivalente di ciò che chiamiamo saldo è in realtà la sommatoria di tutti i valori trasferiti (a credito o a debito) calcolata sulla base della storia di tutte le transazioni effettuate sin dalla prima e che indicherà, in ogni momento, l'effettiva disponibilità di criptoasset non ancora spesi per quell'individuo, mentre l'equivalente di conto è ciò che viene chiamato "wallet", il quale però non assume il significato di contenitore degli asset, bensì di indirizzo di ciascun individuo che ha trasferito criptoasset, al fine di poterne tracciare – e tener tracciato in modo immutabile – ogni scambio avvenuto nel tempo, registrato sul ledger.

15. Nella Blockchain questa prova viene chiamata "Proof-of-Work" e rappresenta il sistema con cui è possibile raggiungere un

consenso distribuito fra più individui su un’unica storia di transazioni.

3

I modelli di governance

Continuando nella presentazione dei personaggi che abitano la nostra immaginaria società, introduciamo ora Grace, un soggetto[16] che rappresenta il Governo e le istituzioni di Welthyland. Grace è in grado di misurare il lavoro compiuto da Trent e di definire la

politica retributiva con cui Trent sarà remunerato. Per esempio, può stabilire una regola per cui Trent sarà ricompensato con 50 Welthy ogni qualvolta annoterà sul libro mastro, validandole, le transazioni in Welthy compiute da Bob, Alice, Charlie, Dan, Erin e così via.

Grace è anche chi istruisce Trent e gli riconosce quella capacità computazionale a fronte di prove difficili che deve portare a termine.

Tutti gli abitanti di Welthyland conoscono le regole su cui Grace[17] si basa per i propri computi e valutazioni e ognuno riconosce legittimità (concetto diverso dalla fiducia) del suo ruolo,

accettandone le decisioni.

Grace, naturalmente, si elegge democraticamente sulla base di un voto espresso da tutti i membri della comunità, ciascuno dei quali ammette, con ciò, che il programma e le regole di Grace siano accettabili e condivise (Figura 3.1).

L'attacco al sistema delle regole e dei controlli

Arriviamo infine a presentare una figura molto sgradevole che, per quanto antipatica e pericolosa, è comunque

presente nella medesima comunità: Mallory, ossia una "entità" in grado di aggredire Trent impedendogli di fare – o anche solo di fare bene – il proprio lavoro.

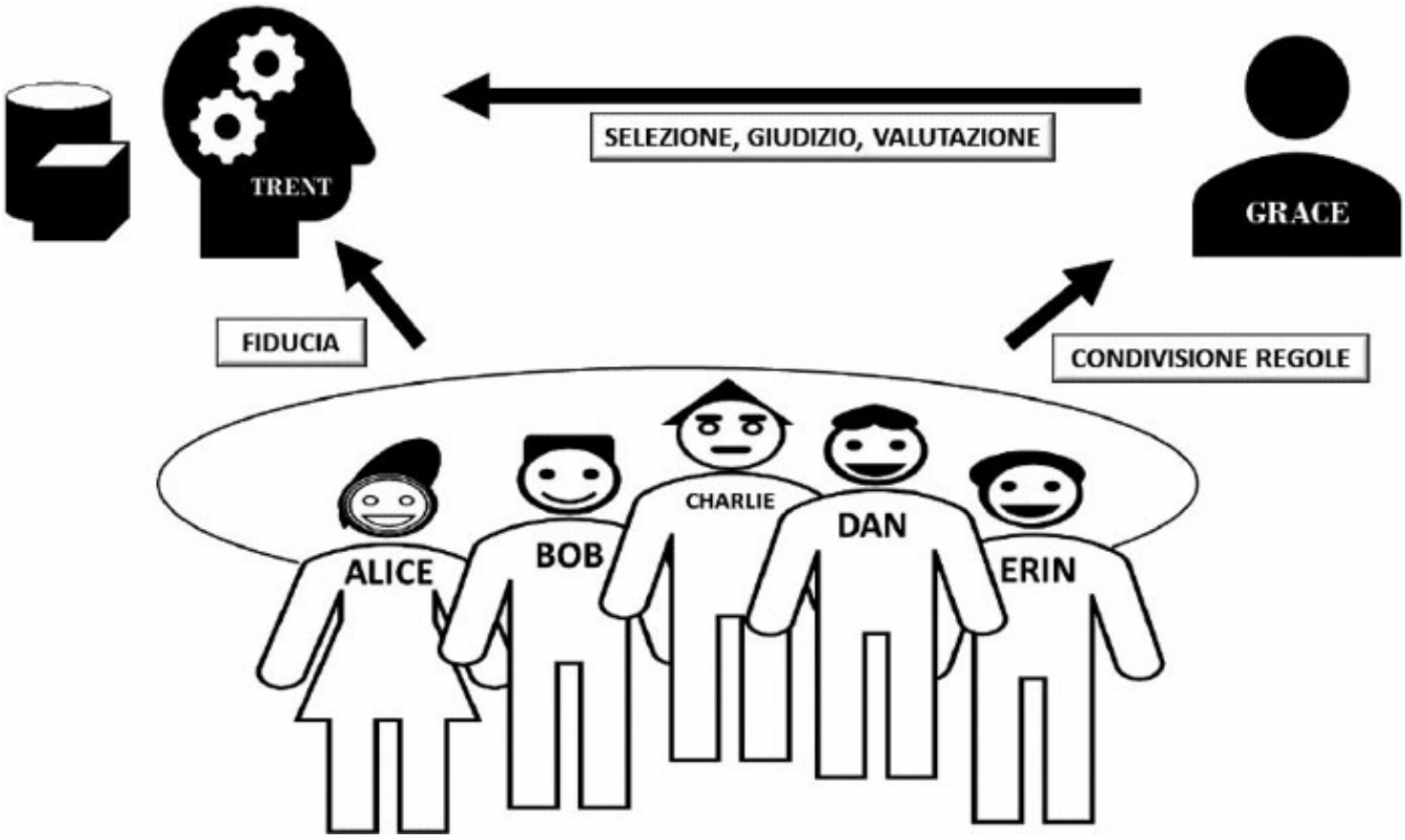

Figura 3.1 – Rapporti di fiducia, condivisione regole e controllo.

Mallory è un'entità che, per definizione, attacca maliziosamente Trent, minandone la credibilità e, in alcuni casi, censurando le sue scelte in forza di un potere che è esterno alla comunità.

Mallory possiede anche una capacità di aggressione endogena; la follia di cui Trent può, a un certo punto, essere vittima, è ben rappresentabile da una "Mallory-malattia" che, distruggendo la sanità mentale del vecchio saggio, gli causerà la sfiducia della società. Mallory è, ovviamente, anche un possibile corruttore che ha buon gioco di Trent, laddove ne conosce i punti deboli. In questo caso, i collaboratori di cui Trent può avvalersi non sono

corruttibili o, meglio, Mallory non spreca energie per corromperli perché, non avendo essi alcun potere se non in subordine a Trent, renderebbero inefficiente qualsiasi sforzo malevolo ordito dall'istigatore. Mallory, quindi, non ha bisogno di energie incommensurate per agire in dolo contro la comunità di Welthyland e artefare la validità degli scambi, gli basta solo avere la meglio su un unico soggetto: Trent.

Mallory, ricordiamocelo bene, essendo parimenti membro della stessa comunità di Welthyland, avrà partecipato all'elezione di Grace. Le relazioni fra Mallory e Grace potranno, in casi estremi, compromettere l'autorità

di Grace. Mallory, infatti, potrebbe chiedere a Grace di cambiare le regole del gioco al fine di modificare le politiche retributive di Trent.

Se Grace, influenzata da Mallory, cambia le regole su cui si basa la remunerazione di Trent, rendendo il suo lavoro inaccettabile, Trent può opporre resistenze che metterebbero a rischio l'intera gestione degli scambi di valore all'interno di Welthyland. Trent potrebbe infatti decidere di annotare le transazioni sul libro mastro molto più lentamente, oppure potrebbe assumere che ogni pagina contabile venga chiusa a intervalli di tempo molto lunghi. In entrambi i casi, inficerebbe

pesantemente il sistema economico (basato sugli scambi) di Welthyland, sotto il profilo prestazionale e quello reputazionale[18] (Figura 3.2).

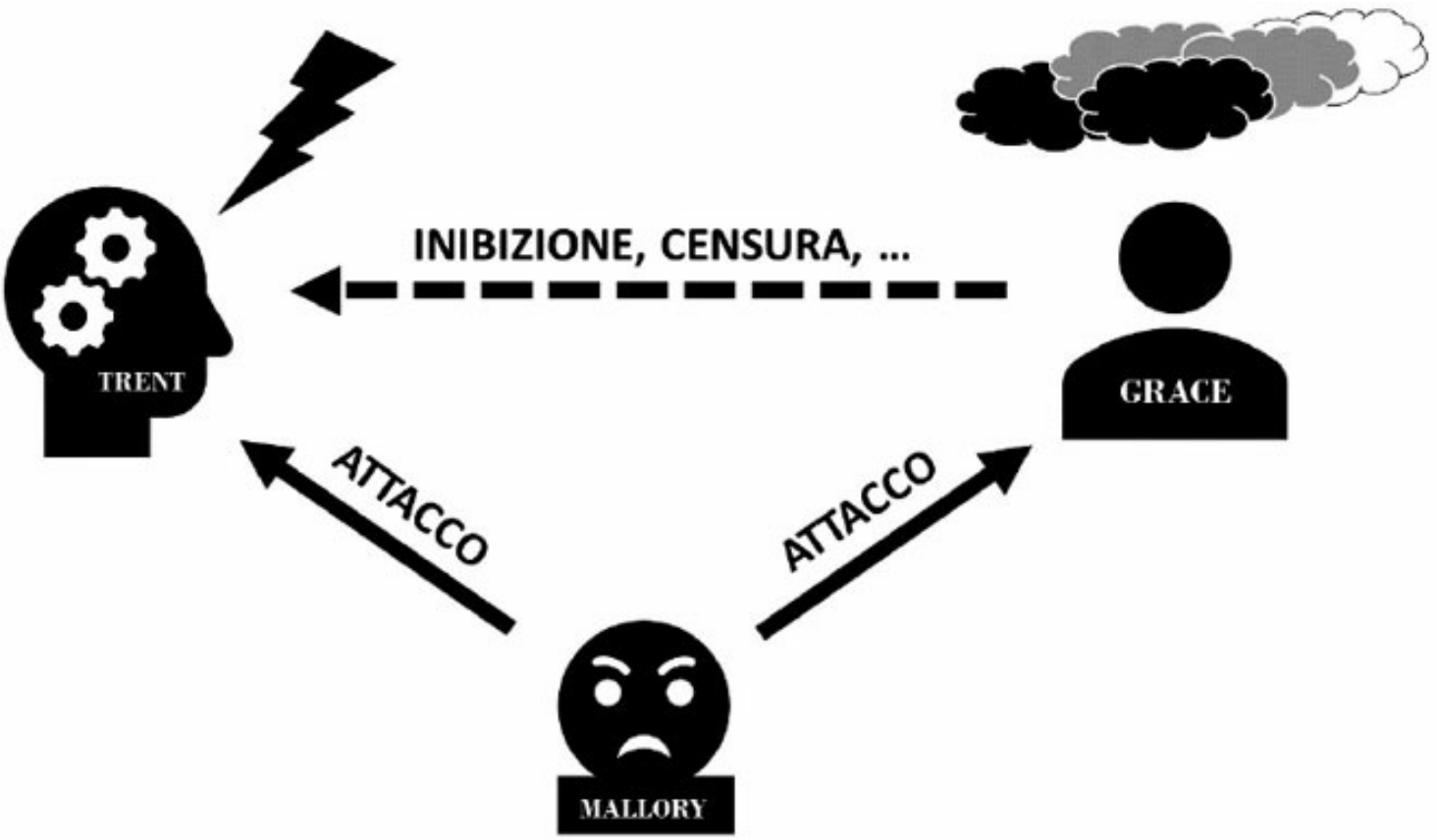

Figura 3.2 – L'attacco al sistema delle regole e dei controlli.

16. Come accennato nel precedente Capitolo 2, Grace non è una singola persona, bensì rappresenta una funzione collettiva, ovvero un'entità preposta all'uopo.

17. Nelle Blockchain pubbliche queste regole sono condivise e accettate da tutti i nodi come nei più diffusi modelli che sono alla base delle comunità di programmatori open source.

18. Nell'analogia con la Blockchain, Mallory rappresenta il nemico che può assumere la personalità di chiunque; può essere per esempio un miner o un gruppo di miner che ha deciso di mettere in comune le forze per sferrare un attacco al sistema, validando blocchi di transazioni surrettiziamente artefatte. Per questo motivo occorre rendere particolarmente oneroso il sistema di validazione dei blocchi tramite la richiesta di Proof-of-Work basata su algoritmi, che devono

essere: resilienti (ossia devono resistere anche di fronte ai possibili cambiamenti esterni imprevedibili), scalabili (non devono costituire possibili colli di bottiglia), noti e condivisi.

4

Le regole del consenso e della fiducia in una blockchain

Al fine di pervenire gradualmente al significato di blockchain più completo, proseguiamo con la nostra storia

fantastica della comunità di Welthyland immaginando che, nel corso degli anni, si susseguano fasi storiche evolutive durante le quali mutano le regole del consenso e della fiducia che ogni abitante adotta per garantire (e vedersi garantita) la bontà degli scambi di Welthy. In ciascuna fase vige un diverso modello su cui la comunità converge per sostenere la propria economia.

Chiameremo questi tre periodi di Welthyland:

1. fase 1 o "periodo del governo centralizzato";
2. fase 2 o "periodo del governo centralizzato e dei controlli distribuiti";

3. fase 3 o “periodo del governo condiviso e del controllo distribuito”.

Modello di governo centralizzato

Nel periodo iniziale (fase 1) a Welthyland esistono solo alcuni individui eletti che hanno il diritto di accedere al mercato e governarne gli scambi. Tali soggetti sono noti a tutti e tutti condividono la scelta di riporre in essi quella fiducia necessaria a garantire gli scambi di Welthy. Non vi è dunque la necessità di inventare un sistema di consensi particolarmente gravoso in

termini di efficienza: la comunità si fida degli eletti e il loro consenso è sufficiente per validare le transazioni di valore. In questa prima fase, per semplificare il racconto e focalizzarci sugli elementi effettivamente distintivi della blockchain, assumiamo che la comunità di Welthyland non si sia volutamente posta il problema di come si possano o debbano produrre i beni oggetto degli scambi, né se si debba porre un limite complessivo alla loro circolazione nella comunità. Sulla base di tale assunto, ogni transazione sarà originata da un membro che dispone sempre di numero sufficiente di Welthy nel proprio patrimonio e l'attestazione di tale disponibilità è sempre data da

quelli stessi individui eletti che governano gli scambi[19].

Modello del governo centralizzato e dei controlli distribuiti

Nella seconda fase l'accesso al mercato, come per la fase 1, è sempre predeterminato; non tutti quindi possono operare senza verifiche preventive e, in particolare, solo coloro che posseggono specifiche caratteristiche possono controllare e dimostrare la correttezza degli scambi e dei cambi di proprietà effettivamente avvenuti. Tali soggetti,

pertanto, come nel periodo del governo centralizzato, saranno preordinatamente indentificati e la comunità riconoscerà in essi una fiducia distribuita. Per contro, la preassegnazione di più soggetti "validatori" decentralizzati implica la necessità di progettare un sistema di consenso altrettanto distribuito (più controllori devono pervenire a un unico risultato) non semplice e che deve essere scalabile per mantenere un sufficiente livello di efficienza.

Modello del governo condiviso e del

controllo distribuito

Nell'ultimo dei tre periodi (la fase 3), i cittadini di Welthyland valutano opportuno porre un limite al numero massimo di Welthy in circolazione, per controllare gli effetti economici. In questo periodo si decide anche una sorta di politica delle attribuzioni (o se preferite delle retribuzioni) che impone l'obbligo di dimostrare un lavoro svolto (più o meno complicato) affinché si possa attribuire la proprietà di un certo quantitativo di Welthy[20].

Welthyland comprende che è possibile consentire l'accesso al mercato senza necessariamente predeterminare alcun vincolo e,

pertanto, chiunque sia in grado di dimostrare alla comunità di aver portato a termine un compito molto complicato ha diritto a venire remunerato in Welthy, che saranno generati come conseguenza del lavoro svolto. Il compito assegnato è, ovviamente, quello di verificare l'esattezza delle transazioni di valore avvenute nella comunità, aggiungendo un'ulteriore richiesta di risoluzione a un enigma crittografico, composto dalle stesse transazioni da validare e da un numero casuale[21]. Come nella fase 2, grazie a questo oneroso meccanismo di verifica che chiunque può adottare, solo pochi individui saranno in grado di presentare la loro prova di lavoro (la

c.d. “Proof-of-Work” o anche “PoW”) corretta, mettendosi in competizione con altri che, per il medesimo fine, ossia quello di vedersi attribuita la proprietà di nuovi Welthy[22], gareggiano. Il sistema dei controlli, diversamente da quello previsto nella fase 2, è un sistema sempre distribuito ma dove i controllori non sono noti (né identificati) *ex ante* da Grace.

Il fatto che non esista più un’autorità centrale e neppure dei controlli distribuiti, non implica, come si potrebbe di primo acchito pensare, che nessuno possa più riporre fiducia in alcuno. Al contrario, se ogni individuo accetta, condividendole, le regole

comuni (governance condivisa) e decide di partecipare alla distribuzione dei controlli (sulla base delle risorse computazionali che dispone a favore della società), la fiducia viene garantita dalla complessità degli algoritmi su cui si basa la dimostrazione della prova di lavoro, che deve essere aggiunta al termine della validazione contabile.

La prova di lavoro è qualcosa molto difficile da produrre ma molto facile da verificare[23]. Si pensi, in analogia, al famoso rompicapo particolarmente diffuso negli anni ’80: il cubo di Rubik. Per risolverlo, al termine del gioco ogni faccia del cubo deve mostrare un solo colore: arrivarci è difficile e ci si

impiega tanto tempo, ma è assolutamente facile per chiunque verificare rapidamente che la soluzione sia stata raggiunta.

In altre parole, chiunque voglia agire in dolo contraffacendo la storia delle transazioni deve competere con tutti gli altri validatori presentando una nuova prova di lavoro costruita sulla verifica di dati transazionali surrettiziamente artefatti, che sia però tale da essere tecnicamente accettabile. Capiremo meglio il significato di questa affermazione nel Capitolo 9, quando spiegheremo tecnicamente come funziona la Blockchain.

In questa terza fase che, per le caratteristiche descritte, chiameremo

“periodo del governo condiviso e del controllo distribuito”, Welthyland è riuscita a riprodurre nel mondo digitale il concetto di scarsità tipica del bene fisico.

Inoltre, Welthyland ha compreso che il sistema adottato per garantire validità e immutabilità delle transazioni in Welthy potrebbe essere anche impiegato al fine di garantire le stesse caratteristiche di sicurezza[24] a qualsiasi altro processo transazionale che avviene al di fuori della proprietà del criptoasset.

La Tabella 4.1 riepiloga cosa accade durante ciascun periodo.

Fasi/modelli	Fiducia	Consenso

1 – Modello del governo centralizzato	Solo in alcuni individui noti e predeterminati è riposta la fiducia della comunità.	Lo scambio di beni viene validato da un'entità centrale senza chiedere il consenso di nessuno.
2 – Modello del governo centralizzato e dei controlli distribuiti	Solo in alcuni individui noti e predeterminati è riposta la fiducia della comunità.	Lo scambio di beni viene validato raggiungendo un consenso distribuito tra più validatori preselezionati.
3 – Modello del governo condiviso e del controllo distribuito	La fiducia è riposta in chiunque dimostri matematicamente di esserne degno, risolvendo un complicato enigma crittografico.	Lo scambio di beni viene garantito e validato raggiungendo un consenso distribuito solo tra chi vuole essere un validatore (potenzialmente

	chiunque potrebbe essere un validatore).

Tabella 4.1 – I tre modelli di governo e controllo.

Siamo ora giunti a un buon livello di comprensione (ne siamo certi) che ci permetterà di analizzare lo scambio dei valori all'interno di Welthyland.

Molti di voi avranno già provato a fare alcune analogie (magari anche grazie alle note a piè di pagina) con ciò che potrebbero aver sentito dire della Blockchain dei Bitcoin (o di altre blockchain) e avranno chiarito qualche dubbio di base. Benissimo! Questa è la strada giusta.

Vediamo adesso cosa può succedere

in ciascuna delle tre fasi storiche di Welthyland, quando Alice e Bob decidono di scambiarsi dei valori, facendo assumere a ciascun abitante della nostra fantastica cittadina il proprio ruolo: Trent è il validatore del libro mastro, Mallory l'attaccante, Grace il governo delle regole.

---

19. Nella fase 1 si è volutamente deciso di non parlare di politica monetaria in quanto, come si vedrà nel seguito, il fine del racconto di Welthyland non è quello di spiegare a chi legge se e come si possa creare, dal nulla, valore monetario da una blockchain.

20. Nella fase 3 qualsiasi deposito di criptoasset sulla Blockchain corrisponde alla ricompensa di un lavoro assegnato, del quale si

è in grado di dimostrare la prova dell'effettiva esecuzione. In altre parole, è possibile entrare nella disponibilità di nuovi Welthy solo a fronte di un lavoro, il cui livello di complessità (che può variare) ha il potere di controllare l'inflazione.

21. Un'analogia che può facilitare la comprensione è rappresentata dal gioco enigmistico dell'anagramma: il validatore deve creare un anagramma che abbia un significato comprensibile a tutti, partendo dalle lettere con cui è descritta la storia delle transazioni sul libro mastro; il livello di difficoltà dell'anagramma può cambiare e, per esempio, può richiedere che il risultato sia composto solo da parole non superiori a cinque lettere, oppure solo da parole che iniziano con una determinata lettera e così via.

22. Nella Blockchain dei Bitcoin il lavoro di validazione delle transazioni viene chiamato

“mining” (nell’analogia con il lavoro, faticoso, di estrazione dell’oro) e i validatori che concorrono a effettuare i controlli, gareggiando nel contempo per risolvere l’enigma crittografico, si chiamano “miner”.

23. La verifica della prova di lavoro offerta dal validatore che per primo risolve l’enigma crittografico deve essere un processo necessariamente rapido e alla portata di tutti, altrimenti, se per verificare l’esattezza della soluzione tutti dovessero effettuare gli stessi calcoli svolti dal validatore vincitore, il sistema non sarebbe affatto efficiente.

24. Questo sistema, come vedremo più avanti nella Parte II del libro, implica considerare il criptoasset che abbiamo chiamato Welthy come una sorta di gettone (o meglio di “token”) che può rappresentare qualsiasi bene materiale oggetto di negoziazione fra parti.

5

Gli scambi di valore nei periodi del governo centralizzato

Immaginiamo che Alice voglia inviare alcuni Welthy a Bob, di cui vanta la proprietà. Chi le ha conferito tale

proprietà? Chi è in grado, in Welthyland, di garantire che Alice abbia realmente un numero sufficiente di Welthy prima di trasferirli a Bob?

Procediamo con ordine. Per dar corso al trasferimento Alice deve:

1. avere precedentemente depositato un numero di Welthy sufficiente;
2. informare Trent che vuole trasferire una parte dei propri Welthy a Bob.

Il deposito di Alice nel periodo del governo

centralizzato

Descriviamo il processo che deve essere eseguito per consentire ad Alice di depositare, supponiamo, 5 Welthy:

1. Alice si reca negli uffici di Trent.
2. Alice saluta Trent (lo conosce perché tutti lo conoscono).
3. Alice chiede a Trent di accettare in deposito 5 Welthy.
4. Trent si accerta che Alice sia realmente chi dice di essere chiedendole un documento

d'identità valido.

5. Trent apre la cassaforte che contiene il libro mastro.

6. Trent annota sul libro mastro il deposito di Alice; da ora in poi Alice dispone di una quantità di Welthy non spesi pari a 5.

7. Trent chiede ad Alice di firmare sul libro mastro che ha effettuato il deposito di 5 Welthy.

8. Trent rilascia una ricevuta di versamento ad Alice firmandola con il proprio nome.

9. Trent ripone il libro mastro nella cassaforte, che poi richiude.

10. Alice esce dagli uffici di Trent certa di aver esperito la corretta procedura che le consentirà di disporre il trasferimento dei suoi Welthy verso Bob.

Avete sicuramente notato come Trent non si sia preoccupato di accertare se, all'atto del deposito, Alice disponesse realmente della quantità di Welthy che voleva depositare. In questa fase 1, infatti, assumeremo che il deposito per Alice (così come per tutti gli altri) avvenga una sola volta nella vita

(magari al compimento della maggior età) e abbia il significato di informare Trent (e, conseguentemente, la comunità tutta) della disponibilità di un bene nella proprietà di Alice (potrebbe essere una dote o un'eredità, oppure semplicemente il frutto dei risparmi dei suoi genitori). Poiché il bene è di proprietà di Alice, la custodia e il riparo dello stesso non è un problema di Trent che, di fatto, nella cassaforte ripone il solo libro mastro che attesta la disponibilità di Alice. Dal momento in cui Alice effettua il suo deposito, può scambiare i suoi Welthy con Bob e qualsiasi altro cittadino di Welthyland. Ogni transazione che effettuerà sarà valida se, prima di iniziarla, disporrà di una quantità di

Welthy non spesi (o non scambiati) sufficiente; tale controllo è garantito dalle scritture contabili sul libro mastro gestito da Trent.

Il trasferimento degli asset di Alice verso Bob nel periodo del governo centralizzato

Bob ha già effettuato il suo primo deposito (come Alice), che supporremo pari a 7 Welthy. Descriviamo ora cosa accade quando Alice vuole trasferire, per esempio, 3 Welthy a Bob:

1. Alice si reca negli uffici di Trent.
2. Alice saluta Trent (lo conosce perché tutti lo conoscono).
3. Alice informa Trent di voler trasferire 3 Welthy del suo patrimonio a Bob.
4. Trent si accerta che Alice sia realmente chi dice di essere chiedendole un documento d'identità valido.
5. Trent chiede le generalità di Bob.
6. Trent apre la cassaforte che contiene il libro mastro.

7. Trent verifica sul libro mastro che la disponibilità di Welthy non spesi da Alice sia tale da permettere il trasferimento verso Bob.

8. Trent annota sul libro mastro che:

    a. Bob dispone ora di 3 Welthy in più di prima, ossia la quantità di Welthy che da ora in poi può spendere è aggiornata 10.

    b. Alice ha una quantità residuale di Welthy non spesi pari a 2.

9. Trent chiede ad Alice di firmare sul libro mastro che ha effettuato il trasferimento di 3 Welthy a Bob.

10. Trent rilascia una ricevuta ad Alice, firmandola con il proprio nome, attestante il fatto che ora Bob ha 3 Welthy in più, frutto del trasferimento a suo favore effettuato da Alice.

11. Trent rilascia ad Alice una seconda ricevuta, firmandola con il proprio nome, attestante il fatto che ora Alice dispone di 2 Welthy non spesi.

12. Alice esce dagli uffici di Trent, prende la prima ricevuta e la trasmette a Bob, di cui conosce l'indirizzo.

13. Quando Bob riceve da Alice la ricevuta prodotta da Trent al punto 10, sa che dispone di nuovi Welthy non spesi e potrà farne utilizzo in qualsiasi momento.

Il lavoro di validazione di Trent

Immaginiamo che nell'arco di 10 minuti si diano 3 transazioni di deposito simili

a quelle descritte per Alice, ma effettuate anche da Charlie ed Erin; per semplicità diremo che ognuno di loro ha depositato la stessa quantità di Welthy, pari a 5.

Sempre nello stesso periodo temporale, sono avvenuti 5 scambi di Welthy simili a quelli descritti per Alice e Bob, tra i seguenti individui[25]:

- Alice → Bob 3 WTH
- Charlie → Erin 7 WTH
- Erin → Alice 2 WTH
- Alice → Charlie 1 WTH
- Dan → Erin 4 WTH

Assumiamo che prima dei 3 depositi e

dei 5 scambi più sopra descritti, Alice, Bob, Charlie, Erin e Dan avessero le seguenti disponibilità di Welthy non spesi:

- Alice = 0 WTH[26]
- Bob = 7 WTH
- Charlie = 15 WTH[27]
- Dan = 4 WTH
- Erin = 5 WTH[28]

Se ordiniamo e identifichiamo[29] le transazioni nel modo[30] mostrato in Tabella 5.1, avremo la variazione delle disponibilità di Welthy non spesi mostrata nella Tabella 5.2.

Al termine dei 10 minuti, Trent fa i

calcoli di contabilità mostrati nella Tabella 5.3 ed è in grado di quadrare i conti relativi all'intervallo di tempo di 10 minuti, intercorso tra l'ultima volta (sicuramente prima delle 12:30:30 del 28/12/17) in cui Trent aveva fatto i medesimi calcoli per l'intervallo temporale precedente e questa volta (le 12:40:30 del 28/12/17). Scriverà questi totali a fine pagina firmandoli e ne aprirà un'altra, pronta ad accogliere le successive annotazioni relative alle transazioni che si compiranno nel successivo arco temporale.

ID Intervallo di tempo n° 1

Data e ora	ID Tx	Transazione
28/12/17 12:30:30	1.1	Alice ↓ 5 WTH

28/12/17 12:30:38	1.2	Charlie ↓ 5 WTH
28/12/17 12:33:02	1.3	Erin ↓ 5 WTH
28/12/17 12:35:58	1.4	Alice → Bob 3 WTH
28/12/17 12:38:38	1.5	Charlie → Erin 7 WTH
28/12/17 12:39:07	1.6	Erin → Alice 2 WTH
28/12/17 12:40:17	1.7	Alice → Charlie 1 WTH
28/12/17 12:40:25	1.8	Dan → Erin 4 WTH

Tabella 5.1 – Ordinamento e identificazione delle transazioni.

ID Intervallo di tempo n° 1

Data e ora	ID Tx	Transazione	Welthy non spesi
28/12/17 12:30:30	1.1	Alice ↓ 5 WTH	Alice = 5 WTH
28/12/17 12:30:38	1.2	Charlie ↓ 5 WTH	Charlie = 20 WTH
28/12/17 12:33:02	1.3	Erin ↓ 5 WTH	Erin = 10 WTH
28/12/17 12:35:58	1.4	Alice → Bob 3 WTH	Bob = 10 WTH I Alice = 2 WTH
28/12/17 12:38:38	1.5	Charlie → Erin 7 WTH	Erin = 17 WTH I Charlie = 13 WTH
28/12/17 12:39:07	1.6	Erin → Alice 2 WTH	Alice = 4 WTH I Erin = 15 WTH
28/12/17 12:40:17	1.7	Alice → Charlie 1 WTH	Charlie = 14 WTH I Alice = 3 WTH
28/12/17 12:40:25	1.8	Dan → Erin 4 WTH	Erin = 19 WTH I Dan = 0 WTH

Tabella 5.2 – Disponibilità non spese.

	Dare	Avere	Welthy non spesi in precedenza	Welthy non spesi
Alice	3 + 1 = 4 WTH	5 + 2 = 7 WTH	0	0 + (7 – 4) = 3 WTH
Bob	0 WTH	3 WTH	7	7 + (3 – 0) = 10 WTH
Charlie	7 WTH	6 WTH	15	15 + (6 – 7) = 14 WTH
Dan	4 WTH	0 WTH	4	4 + (0 – 4) = 0 WTH
Erin	2 WTH	5 + 7 + 4 = 16 WTH	5	5 + (16 – 2) = 19 WTH

Tabella 5.3 – Contabilizzazioni parziali.

Grace ha stabilito una regola (condivisa dalla comunità di Welthyland) in ordine alla quale Trent avrà diritto a disporre di un certo numero fisso di Welthy – supponiamo 50 – e di una quota parte variabile in funzione delle quantità di

valori che sono stati scambiati nell'intervallo di tempo in esame. Quindi, sulla base del lavoro condotto da Trent durante gli ultimi 10 minuti e al termine dei calcoli che scriverà, firmandoli, a fine pagina, viene calcolata una retribuzione per Trent, che gli permette di continuare a fare il suo lavoro con soddisfazione.

Un modo alternativo per controllare la reale disponibilità di Welthy non spesi

Trent è in grado di sapere, guardando il libro delle contabilizzazioni, tutta la storia di tutte le transazioni di ogni membro della comunità di Welthyland avvenute sino a quel momento. Prendiamo per esempio Alice, la cui disponibilità di Welthy aggiornata al termine dei 10 minuti in esame è pari a 3 WTH. Trent è in grado di dimostrare che questa quantità di Welthy è nella disponibilità di Alice, in quanto frutto delle transazioni avvenute nel corso degli ultimi 10 minuti (mostrate nella Tabella 5.4).

Storia delle transazioni di Alice

Time	Tx	Amount	Tx ID	Input (da chi ha ricevuto Welthy)	Output (verso chi ha trasmesso Welthy)
28/12/17 12:30:30	*Deposito*	5 WTH	1.1	Alice	Alice
28/12/17 12:35:58	*Trasmesso*	3 WTH	1.4	Alice	Bob
28/12/17 12:39:07	*Ricevuto*	2 WTH	1.6	Erin	Alice
28/12/17 12:40:17	*Trasmesso*	1 WTH	1.7	Alice	Charlie
	Welthy non spesi	3 WTH			

Tabella 5.4 – Storia delle transazioni.

Quindi, un altro modo per riportare la disponibilità in Welthy non ancora spesa di Alice potrebbe essere anche quello mostrato nella Tabella 5.5.

	Dare	Avere	Welthy non spesi in precedenza	3 Welthy non spesi
Alice	3 + 1 = 4 WTH	5 + 2 = 7 WTH	0	

Time	Tx	Amount	Tx ID	Input (da chi ha ricevuto Welthy)	Output (verso chi ha trasmesso Welthy)
28/12/17 12:30:30	*Deposito*	5 WTH	1.1	Alice	Alice
28/12/17 12:35:58	*Trasmesso*	3 WTH	1.4	Alice	Bob
28/12/17 12:39:07	*Ricevuto*	2 WTH	1.6	Erin	Alice
28/12/17 12:40:17	*Trasmesso*	1 WTH	1.7	Alice	Charlie

Tabella 5.5 – Modalità alternativa per il

computo delle disponibilità non spese.

Similmente si potrebbe fare per le altre disponibilità movimentate, nell'intervallo di tempo in questione, da Bob, Charlie, Dan ed Erin, costruendo altrettante tabelle nidificate.

Un modo per verificare l'effettiva disponibilità di Welthy di ognuno potrebbe dunque essere quella di chiedere a Trent di verificare la storia di tutte le transazioni compiute da ciascun individuo, prima di approvare qualsiasi scrittura sul libro contabile.

Accantoniamo, per ora, questa riflessione che ci tornerà utile quando parleremo delle successive fasi 1 e 2 di Welthyland, ma poniamoci alcune

domande: in questa fase della nostra immaginaria società che abbiamo chiamato "periodo del governo centralizzato", che cosa rende possibile ad Alice di disporre con certezza del patrimonio non ancora speso pari a 3 WTH alle ore 12:40:17 del 28/12/17? Oppure, chi tutela Erin al fine di garantirle che alle 12:38:38 del 28/12/17 abbia realmente a disposizione 17 WTH da spendere?

La risposta è piuttosto semplice, anche se non così scontata: la sequenza con cui sono state annotate le transazioni contabili garantisce, in ogni momento, l'effettiva bontà degli scambi. Trent o, meglio, il lavoro di Trent per cui Grace ha stabilito che venga remunerato,

assicura l'economia di scambi su cui Welthyland si basa.

Gli scambi di valore nel periodo del governo centralizzato e dei controlli distribuiti

A partire questa fase inizieremo a far emergere alcune caratteristiche che, al di là dell'analogia narrata con il racconto di Welthyland, sono tipiche della Blockchain (o meglio, delle blockchain[31]).

Differentemente dal periodo precedente, Welthyland comprende quanto sia utile che Trent non resti una figura sola e unica[32] e che sia possibile individuare più soggetti di pari grado capaci di svolgere il ruolo di detentori e validatori del libro mastro. Si incarica dunque Grace di selezionare preventivamente gli equipollenti di Trent, ai quali conferisce il potere di mantenere una copia del libro mastro su cui ognuno di loro provvederà a fare i propri calcoli e a firmarne il risultato.

La necessità di avere più duplicati del libro delle transazioni implica si adotti un meccanismo di replica che, a ogni nuova transazione, aggiorni tutte le

copie. Per fare depositi e trasferimenti, Alice e Bob (e tutti gli altri) potranno rivolgersi a un qualsiasi Trent degli "n" distribuiti, avendo la stessa garanzia che ricevevano nella fase 1 di Welthyland.

Il fatto che vi siano più validatori che operano contemporaneamente sulla medesima copia di transazioni richiede il raggiungimento di un accordo comune sull'esito dei calcoli che vengono fatti al termine di ogni pagina. Non solo; è importante anche capire chi possa decidere di definire l'intervallo di tempo (i famosi 10 minuti della fase 1) alla chiusura del quale partono i processi di validazione contabile. In una siffatta situazione è richiesto un consenso distribuito fra gli "n" Trent,

che possa determinare un'unica verità circa la storia delle transazioni.

Rispetto alla fase 1, inoltre, non esiste più il concetto di cassaforte gestita da un singolo Trent. Ciò non significa che non esista più in quanto luogo unico e sicuro: al contrario, la sicurezza con cui il solo Trent custodiva nella cassaforte l'unica copia del libro mastro nella fase 1 ora è distribuita preso gli "n" validatori che operano sulle "n" copie del libro mastro replicato.

Rivediamo dunque sia il deposito di Alice sia lo scambio con Bob in questo periodo che abbiamo chiamato "del governo centralizzato e dei controlli

distribuiti”.

Il deposito di Alice nel periodo del governo centralizzato e dei controlli distribuiti

Descriviamo il processo che deve essere eseguito per consentire ad Alice di depositare, supponiamo, 5 Welthy:

1. Alice si reca negli uffici del Trent più vicino.
2. Alice saluta Trent (lo conosce perché tutti lo

conoscono).

3. Alice chiede a Trent di accettare in deposito 5 Welthy.

4. Trent si accerta che Alice sia realmente chi dice di essere chiedendole un documento d'identità valido.

5. Trent accede in sicurezza alla copia del libro mastro in suo possesso.

6. Trent annota sul libro mastro il deposito di Alice.

7. Trent chiede ad Alice di firmare sul libro mastro che ha effettuato il deposito di 5

Welthy.

8. Trent rilascia una ricevuta di versamento ad Alice firmandola con il proprio nome.

9. Trent replica la scrittura del libro mastro relativa al deposito di Alice inviandola agli altri Trent di cui conosce le generalità.

10. Alice esce dagli uffici di Trent convinta di aver esperito la corretta procedura che le consentirà di disporre il trasferimento dei suoi Welthy verso Bob.

Avete sicuramente notato come, rispetto alla fase 1, al termine della procedura Alice non sia *certa* bensì solo *convinta* che il suo deposito sia già stato confermato da Trent. In realtà Trent non è più il solo e unico custode della verità e deve attendere che anche gli altri validatori (coloro che agiscono sulle copie del libro contabile) acconsentano di aggiornare la storia delle transazioni, inserendo quella di Alice.

Il trasferimento degli asset di Alice verso Bob nella fase 2

Descriviamo ora cosa accade quando Alice vuole trasferire, per esempio, 3 Welthy a Bob:

1. Alice si reca negli uffici del Trent più vicino.
2. Alice saluta Trent (lo conosce perché tutti lo conoscono).
3. Alice informa Trent di voler trasferire 3 Welthy del suo patrimonio a Bob.
4. Trent si accerta che Alice sia realmente chi dice di essere chiedendole un documento d'identità valido.
5. Trent chiede le generalità di

Bob.

6. Trent accede in sicurezza alla copia del libro mastro in suo possesso.

7. Trent verifica sul libro mastro che la disponibilità di Welthy non spesi da Alice sia tale da permettere il trasferimento verso Bob: fa questa operazione ripercorrendo a ritroso la storia delle transazioni originate da Alice come abbiamo visto nel paragrafo: “Un modo alternativo per controllare la reale disponibilità di Welthy non

spesi” di questo stesso capitolo.

8. Trent annota sul libro mastro che:

a. Bob dispone ora di 3 Welthy in più di prima, ossia la quantità di Welthy che può spendere è aggiornata 10.

b. Alice ha una quantità residuale di Welthy non spesi pari a 2.

9. Trent chiede ad Alice di firmare sul libro mastro che ha effettuato il trasferimento

di 3 Welthy a Bob.

10. Trent rilascia una ricevuta ad Alice, firmandola con il proprio nome, attestante il fatto che ora Bob ha 3 Welthy in più, frutto del trasferimento a suo favore effettuato da Alice.

11. Trent rilascia ad Alice una seconda ricevuta, firmandola con il proprio nome, attestante il fatto che ora Alice dispone di 2 Welthy non spesi.

12. Trent replica la scrittura del libro mastro relativa al trasferimento di Alice verso

Bob inviandola agli altri Trent di cui conosce le generalità.

13. Alice esce dagli uffici di Trent, prende la prima ricevuta e la trasmette a Bob, di cui conosce l'indirizzo.

14. Quando Bob riceve da Alice la ricevuta prodotta da Trent al punto 10, è convinto di poter disporre di nuovi Welthy non spesi.

Anche in questo caso avete sicuramente notato come, rispetto alla fase 1, al termine della procedura Bob non sia *certo* bensì solo *convinto* che il

trasferimento di Welthy a suo beneficio sia già stato confermato da Trent. In realtà Trent non è più il solo e unico custode della verità e deve attendere che anche gli altri validatori (coloro che agiscono sulle copie del libro contabile) acconsentano di aggiornare la storia delle transazioni, inserendo quella relativa al trasferimento di Alice verso Bob.

Il lavoro di validazione dei Trent nel periodo del governo centralizzato e dei

controlli distribuiti

Come per la fase 1, consideriamo validi i ragionamenti fatti in merito ai depositi e ai trasferimenti avvenuti nell'arco temporale di 10 minuti e arriviamo subito all'analisi di quanto succede al libro mastro.

Ciò che mostriamo qui di seguito è la storia delle transazioni avvenute tra le 12:30:30 del 28/12/17 e le 12:39:07 del 28/12/17 secondo Trent(i), intendendo con questa dicitura riferirci a un generico Trent fra quelli che Grace ha individuato e ai quali ha assegnato il compito di validazione delle transazioni. Nella fattispecie Trent(i) è il Trent presso il quale Alice ha depositato e

trasferito Welthy. Poiché ciascun Trent possiede una copia del libro mastro replicato, identificheremo la struttura che segue come l'immagine che ritiene di avere il Trent presso cui si sono esperite le transazioni di Alice, in un intervallo di tempo che ha misurato con il suo orologio (che potrebbe non essere sincronizzato con quello degli altri validatori). Per evidenziare meglio questo concetto, riportiamo in corsivo le transazioni che non sono avvenute presso gli uffici di Trent(i), ma di cui Trent(i) ha visibilità in quanto repliche (Tabella 5.6).

Copia del libro mastro esaminata da Trent(i)

ID Intervallo di tempo n° i.1			
Data e ora	ID Tx	Transazione	Welthy non spesi
28/12/17 12:30:30	1.1	Alice ↓ 5 WTH	Alice = 5 WTH
28/12/17 12:30:38	*1.2*	*Charlie ↓ 5 WTH*	*Charlie = 20 WTH*
28/12/17 12:33:02	*1.3*	*Erin ↓ 5 WTH*	*Erin = 10 WTH*
28/12/17 12:35:58	1.4	Alice → Bob 3 WTH	Bob = 10 WTH I Alice = 2 WTH
28/12/17 12:38:38	*1.5*	*Charlie → Erin 7 WTH*	*Erin = 17 WTH | Charlie = 13 WTH*
28/12/17 12:39:07	*1.6*	*Erin → Alice 2 WTH*	*Alice = 4 WTH | Erin = 15 WTH*
28/12/17 12:40:17	1.7	Alice → Charlie 1 WTH	Charlie = 14 WTH I Alice = 3 WTH
28/12/17 12:40:25	*1.8*	*Dan à Erin 4 WTH*	*Erin = 19 WTH | Dan = 0 WTH*

Tabella 5.6 – Parziale del libro mastro.

Al termine dei 10 minuti, se Trent(i) volesse avere contezza della storia delle transazioni che hanno riguardato Alice, vedrebbe quanto mostrato in Tabella 5.7.

La disponibilità aggiornata di Alice è frutto di tre transazioni per le quali Trent(i) l'ha identificata di persona (1.1, 1.4, 1.7) ma vi è anche una transazione, la 1.6, per la quale si deve fidare della replica. Erin, infatti, sarà stata

identificata da un altro Trent che chiameremo Trent(i+1), il quale avrà provveduto ad aggiornare la propria copia del registro, scrivendo che da Erin sono stati trasferiti, a beneficio di Alice, 2 Welthy.

Copia del libro mastro esaminata da Trent(i)

ID Intervallo di tempo n° i.1									
	Dare	Avere	Welthy non spesi in precedenza	3 Welthy non spesi					
Alice	3 + 1 = 4 WTH	5 + 2 = 7 WTH	0	Time	Tx	Amount	Tx ID	Input (da chi ha ricevuto Welthy)	Output (verso chi ha trasmesso Welthy)
				28/12/17 12:30:30	Deposito	5 WTH	1.1	Alice	Alice
				28/12/17 12:35:58	Trasmesso	3 WTH	1.4	Alice	Bob
				28/12/17 12:39:07	*Ricevuto*	*2 WTH*	*1.6*	*Erin*	*Alice*
				28/12/17 12:40:17	Trasmesso	1 WTH	1.7	Alice	Charlie

Tabella 5.7 – Storia delle transazioni.

Per avere la garanzia che tutte le transazioni compiute negli intervalli di

tempo siano valide, è necessario raggiungere un consenso distribuito tra i diversi validatori su un'unica verità. Le regole di come si debba pervenire a tale consenso[33] sono state definite ovviamente da Grace (con l'approvazione dell'intera comunità di Welthyland) e l'accettazione da parte di tutti i Trent che, ricordiamo, sono tutti individuati da Grace.

---

25. Per convenzione assumiamo che il Welthy, quando deve indicare una quantità che viene depositata o trasferita, si abbrevi con la sigla WTH.

26. Alice non aveva mai fatto alcun deposito, il suo primo deposito si è dato durante i 10 minuti dell'arco temporale in esame.

27. Charlie, prima di effettuare il suo primo deposito durante i 10 minuti dell'arco temporale in esame, aveva ricevuto da altri membri di Welthyland una quantità di Welthy non spesi pari a 15.

28. Erin, prima di effettuare il suo primo deposito durante i 10 minuti dell'arco temporale in esame, aveva ricevuto da altri membri di Welthyland una quantità di Welthy non spesi pari a 5.

29. L'identificativo della transazione è così formato: X.Y, dove X identifica l'intervallo di riferimento entro cui sono avvenute le transazioni e Y identifica la posizione della singola transazione nell'intervallo temporale in esame.

30. Il simbolo â indica un deposito; il simbolo à indica un trasferimento.

31. Si veda il box "Blockchain e Bitcoin: attenzione a come sono scritte le iniziali".

32. Rimandiamo al successivo capitolo per una analisi SWOT puntuale che mostri pregi e difetti di una soluzione basata su un ledger centralizzato come quello adottato nella fase 1, sulla base della quale si comprenderanno le ragioni a sostegno di un modello basato su controlli distribuiti quale è quello che viene descritto in questo paragrafo.

33. Tra le diverse tecniche per raggiungere questo consenso usate in alcune tipologie di blockchain private – come Hyperledger – o ibride – per esempio Ripple – figurano rispettivamente PBFT (Practical Byzantine Fault Tolerance) e RPCA (Ripple Protocol Consensus Algorithm).

6

Gli scambi di valore nel periodo del governo condiviso e del controllo distribuito

Arriviamo ora alla fase in cui

Welthyland decide che sia opportuno liberare l'accesso al mercato degli scambi, consentendo a chiunque di detenere una copia del libro mastro sul quale potrà validare le transazioni, in concorrenza – quasi perfetta[34] – con qualunque altro membro della comunità.

Differentemente dal periodo del governo centralizzato e da quello del governo centralizzato e dei controlli distribuiti, Welthyland comprende l'utilità che Trent possa essere ogni singolo individuo a patto che accetti le regole di una "Grace decentralizzata". Cosa intendiamo con questa affermazione? Che chiunque può essere Trent e Grace? Precisiamo meglio.

Chiunque ha il diritto ad assumere il ruolo di Trent a patto che accetti le regole condivise (o il protocollo condiviso) con la comunità, esattamente come accade nelle comunità di programmatori open source. Tutti quindi possono vedere le transazioni di tutti, così come ognuno può concorrere alla verifica delle stesse e alla validazione delle pagine contabili che raggruppano le transazioni verificate. In questo modo la fiducia non deve essere riposta in Trent e in Grace ma, poiché chiunque ha la possibilità di verificare e validare la storia delle transazioni di tutti, la fiducia sarà riposta in un algoritmo che permetterà di raggiungere un consenso distribuito anche fra individui che tra di

loro non si conoscono e che, pertanto, potrebbero a buon diritto ritenere di non fidarsi.

Cosa significa verificare una transazione e validare una pagina di transazioni verificate

Per comprendere il modello che Welthyland ha adottato in questa fase, ovvero per capire esattamente cosa sia la Blockchain, è opportuno distinguere due concetti apparentemente simili nelle

situazioni raccontate per le fasi precedenti, ma molto diversi in questo periodo che abbiamo chiamato del governo condiviso e del controllo distribuito:

- verifica di una transazione di scambio in Welthy;
- validazione delle pagine contabili che includono le transazioni di scambio verificate.

La verifica delle transazioni avviene da qualsiasi membro della comunità di Welthyland che agisce sul libro mastro replicato e si compone di tre momenti specifici, sincroni per ciascun membro:

1. verifica della validità della richiesta di effettuazione di una transazione, ossia accertamento del soggetto che intende trasferire Welthy;
2. verifica della effettiva disponibilità di Welthy non spesi tramite l'analisi a ritroso di tutte le transazioni effettuate dal soggetto identificato;
3. inserimento della transazione verificata in una pagina contabile del libro mastro distribuito.

La validazione delle pagine contabili

inclusive delle transazioni verificate implica che i membri volonterosi di assurgere al ruolo di validatori sappiano fare alcuni calcoli matematici molto complicati e onerosi in termini energetici (devono possedere grandi capacità computazionali).

La validazione delle pagine contabili di un registro distribuito

I membri che vogliono concorrere alla validazione delle pagine (o blocchi, se preferite…) si assumono una grande responsabilità: garantire l'ordine delle

transazioni verificate.

Non dimentichiamoci che siamo in un ambiente distribuito dove l'inserimento di una transazione verificata da un membro non si propaga istantaneamente e dove pertanto può capitare che alcuni membri della comunità non riescano a inserire nelle stesse pagine contabili le transazioni verificate da altri. Se qualcuno (o qualcosa) di particolarmente veloce, che individueremo in Mallory, riuscisse a creare una pagina all'interno della quale altera l'ordine con cui si sono verificate le transazioni verificate, potrebbe propagare liberamente l'informazione surrettiziamente modificata a tutti gli altri che non saprebbero quale

considerare buona, rischiando di validare una storia non vera.

La prova di lavoro per la validazione delle pagine di un registro distribuito

Per complicare l'esistenza di Mallory occorre dunque che il procedimento di validazione sia molto costoso, al fine di dissuaderlo nel perpetrare il suo atto criminoso. Inoltre, è necessario mettere in concorrenza tutti i membri che vogliono validare le pagine contabili del

registro distribuito, promettendo loro una ricompensa.

Ciò si rende possibile grazie a un algoritmo che definisce un complicato enigma matematico molto simile al gioco dell'anagramma, nel quale è come se le parole da analizzare corrispondessero alle transazioni incluse nelle pagine contabili del libro mastro distribuito e il risultato cui si debba pervenire fosse una frase di senso compiuto (tale cioè da poter essere verificata da tutti rapidamente). Il validatore deve creare un anagramma partendo dalle lettere con cui è descritta la storia delle transazioni verificate sul libro mastro; il livello di difficoltà dell'enigma può cambiare e, per

esempio, può richiedere che il risultato sia composto solo da parole non superiori a cinque lettere, oppure solo da parole che iniziano con una determinata lettera e così via. Tali regole cambiano ciclicamente sulla base di regole condivise dalla comunità.

Ogni pagina è numerata e contiene un riferimento all'ultima pagina che è stata validata da un precedente validatore, creando in questo modo una catena di pagine (o di blocchi, se preferite…) contenenti la storia di tutte le transazioni in Welthy verificate e validate.

Per ricompensare il lavoro del validatore ogni pagina di transazioni contiene un premio, sempre espresso in

Welthy. Nel momento in cui il validatore Dan (per fare un esempio) risolve l'anagramma, ha diritto a vedersi depositati quei Welthy di ricompensa; sulla copia del libro mastro in cui è presente la pagina validata da egli stesso comparirà una transazione di deposito simile a quella descritta nei precedenti paragrafi per Alice, Charlie ed Erin. Una volta che tale pagina (con la transazione di ricompensa assegnata a Dan per aver risolto il gioco) viene replicata per tutti gli altri, ognuno può verificare la correttezza della soluzione e agganciare la pagina che Dan ha validato alle precedenti, allungando di fatto la catena.

Ciascun membro che si candida a

validare le pagine guarda come deve essere composto l'anagramma da creare; ognuno ne ha evidenza perché viene veicolato insieme alla catena delle pagine validate in precedenza. Ciascun validatore effettua le sue prove agendo sulle transazioni che si sono originate, supponiamo, negli ultimi 10 minuti, includendo nei propri calcoli la soluzione dell'anagramma – anch'esso scritto nel registro – trovata dal precedente validatore e relativo alla precedente pagina validata (in questo modo si ha la garanzia della concatenazione di prove sulle pagine verificate anteriormente). Nel fare questa attività ognuno deve

anagrammare le transazioni che sta verificando cercando di pervenire il più rapidamente possibile alla soluzione richiesta; tale esercizio costituisce la prova del lavoro fatto da ciascun verificatore delle transazioni. Poiché richiede molta energia (risorsa naturale scarsa), ognuno è incentivato ad arrivare per primo, volendo essere legittimato a ottenere la ricompensa.

Il problema del "Double Spending"

Qualora il "validatore Mallory" volesse alterare la storia delle transazioni, magari duplicando una o più transazioni,

dovrebbe competere con tutti gli altri membri del gruppo, riuscendo a ricreare una catena che includa la transazione fittizia ma, per fare ciò, dovrebbe ricalcolare molto velocemente tutti gli anagrammi che sono stati prodotti e risolti dagli altri validatori sulla catena di transazioni contabilizzate, al fine di imporre come "buona" la sua catena.

Questo fatto, sulla Blockchain dei Bitcoin, potrebbe essere teoricamente realizzabile laddove il malintenzionato riuscisse, in un determinato istante, a possedere il 51% della potenza di calcolo di tutti gli altri validatori.

La ricompensa dei validatori delle pagine di un registro distribuito

In questa fase 3 di Welthyland, lo ricordiamo, si è deciso che l'unica possibilità per effettuare un deposito in Welthy è rappresentata dalla ricompensa che al validatore vincitore del gioco enigmistico è riconosciuta. Inoltre, al fine di programmare l'inflazione, la nostra immaginaria comunità che abbiamo scelto di raccontare per spiegare la Blockchain si è data un limite alla disponibilità di Welthy,

decidendone un numero massimo in circolazione. Infatti, la ricompensa può essere dimezzata a intervalli di tempo precostituiti (per esempio ogni "n" anni, dove "n" è una regola condivisa da tutti).

Ma non è solo questo il sistema che può controllare efficacemente l'inflazione. La difficoltà dell'anagramma, abbiamo detto, può essere modificata e, supponiamo, che ciò avvenga ogni 2.016 pagine validate. Se – almeno in linea teorica – ogni validatore fosse in grado di mostrare la Proof-of-Work mediamente ogni 10 minuti, per validare 2.016 pagine sarebbero necessarie 2 settimane.

Qualora si avesse una frequenza di validazione molto più bassa e il numero di depositi diminuisse, la comunità potrebbe decidere di diminuire la difficoltà dell'anagramma riportando l'economia degli scambi su cui si basa Welthyland a livelli di efficienza accettabili. Al contrario, se il numero di depositi aumentasse, per via del fatto che i validatori sono molto più veloci nel trovare la soluzione, la comunità potrebbe decidere di incrementare il livello di difficoltà dell'enigma.

Le transazioni sul registro distribuito

Per comprendere meglio questi meccanismi, rifacciamo lo stesso esercizio svolto per descrivere cosa accadeva quando Alice trasferiva 3 Welthy a Bob nelle fasi 1 e 2 di Welthyland, nell'ipotesi che sia Dan il soggetto validatore risolutore dell'enigma.

1. Alice accede in sicurezza alla copia del libro mastro in suo possesso.
2. Alice verifica sulla sua copia locale del libro mastro che la disponibilità di Welthy non spesi sia tale da permettere il trasferimento verso Bob.

3. Alice scrive sul libro mastro che:

    a. Bob dispone ora di 3 Welthy in più di prima, ossia la quantità di Welthy che può spendere è aggiornata 10.

    b. Alice ha una quantità residuale di Welthy non spesi pari a 2.

4. Alice firma, sulla sua copia locale del libro mastro, che ha effettuato il trasferimento di 3 Welthy a Bob.

5. Alice replica la scrittura del

libro mastro relativa al trasferimento che ha effettuato verso Bob inviandola agli altri membri della comunità.

6. Ciascun membro della comunità (incluso Bob) verifica l'identità di Alice poiché ciascuno riconosce la firma di Alice.

7. Ciascun membro della comunità (incluso Bob) verifica l'effettiva disponibilità di Welthy non spesi di Alice prima del trasferimento a Bob, andando a verificare a ritroso tutte le transazioni effettuate da

Alice.

8. Ciascun membro (compreso Bob) include la transazione verificata nella successiva pagina contabile da validare.

9. Quando Bob vede sulla sua copia del libro mastro che la sua disponibilità in Welthy non spesi è aumentata grazie al trasferimento di Alice (verificato da tutti), è convinto di poter disporre di nuovi Welthy non spesi ma, in realtà, quella transazione deve essere ancora confermata dal primo validatore che risolverà

l’anagramma.

10. I membri che si candidano a essere validatori delle pagine contabili – la prossima delle quali sarà inclusiva anche della transazione verificata di Alice verso Bob – iniziano la gara per risolvere l’anagramma associato alla pagina da validare.

11. Dan è il primo a risolvere l’enigma e lo comunica a tutti gli altri validatori, propagando la sua prova di lavoro.

12. Ciascun validatore controlla che l’anagramma prodotto da

Dan sia effettivamente stato creato come richiesto e aggancia alla catena delle pagine contabili validate in precedenza la nuova pagina validata da Dan, inserendo un riferimento a quella immediatamente precedente.

13. Dan ha diritto di vedersi riconosciuta la ricompensa in Welthy prevista in quella pagina.

Domanda: sarà sufficiente per Bob una sola conferma (ossia la validazione fatta dal vincitore Dan) perché gli sia garantita l'effettiva disponibilità dei Welthy ricevuti da Alice?

Prima di rispondere tenete in conto che siamo in una situazione dove il libro mastro è distribuito fra tutti e, pertanto, la propagazione delle repliche non può essere immediata. Per esempio, Erin potrebbe avere visibilità della transazione compiuta da Alice verso Bob in un momento successivo a quello in cui Dan ha mostrato la sua prova di lavoro e, in tal senso, potrebbe concorrere alla soluzione del nuovo enigma solo verificando una pagina nuova – inclusiva della transazione di Alice – perché quella precedente è stata già chiusa da Dan.

Una simile situazione potrebbe verificarsi anche per Charlie, così come

per gli stessi Alice e Bob. Buona norma vuole quindi che, per avere una sufficiente garanzia dei Welthy ricevuti da Alice, Bob attenda almeno altre 6 conferme (quindi teoricamente almeno 1 ora). In altre parole, più la transazione di Alice verso Bob si trova in una posizione arretrata della catena (ovvero più la catena è formata da un numero di blocchi consistenti) maggiore è la probabilità che Bob veda garantita la sua nuova disponibilità di Welthy non spesi ricevuti da Alice.

Cosa potrebbe accadere nel caso di

“Double Spending”

Ipotizziamo che Mallory, complice Alice, riesca a possedere il 51% della potenza di calcolo dell’intera comunità di Welthyland, nel momento in cui compie la sua truffa[35].

Mallory sarebbe in grado di decidere arbitrariamente quali transazioni possano realmente aver luogo, permettendo ad Alice, per esempio, di riaccreditarsi la medesima quantità di Welthy appena trasferiti a Bob. In che modo? Semplicemente chiedendo ad Alice la chiave privata per firmare le transazioni (Alice è sua complice e quindi ci sta), scrivendo la transazione fittizia sulla copia locale del

libro mastro a cui accede e subito dopo validandosela, ovvero prima che altri possano validare la pagina che contiene la transazione di Alice a beneficio di Bob: in quell'istante Mallory possiede la maggiore capacità computazionale, pertanto può tranquillamente perpetrare l'azione poiché gli altri validatori sono bloccati. Questa situazione, per quanto teorica, viene descritta nella Figura 6.1, dove abbiamo riportato per semplicità i soli riferimenti alle azioni descritte nella precedente lista ed evidenziato l'attacco "del 51%" inserendolo nell'area delimitata dalla linea tratteggiata.

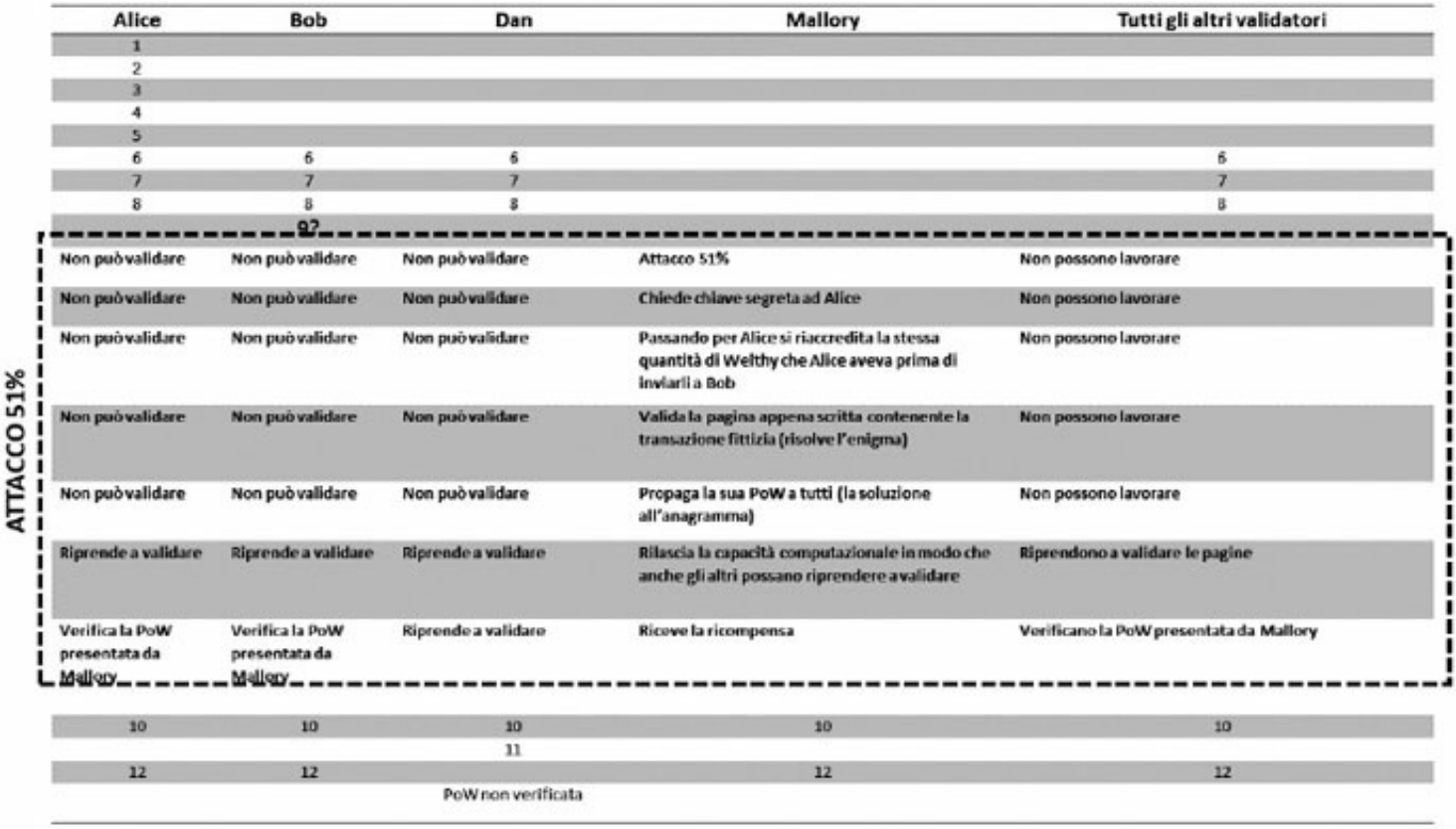

Figura 6.1 – Simulazione attacco "del 51%".

In questo caso, avrete notato che Mallory non solo perpetra il reato per conto di Alice (dalla quale poi, probabilmente, si farà ricompensare… ma questo non rileva ai fini della spiegazione) ma incassa anche (e subito) l'incentivo per aver validato il proprio

blocco.

Gli incentivi per i validatori delle transazioni su un registro distribuito

Nella terza fase di Welthyland (come per la fase 1) le regole accettate dalla comunità prevedono che la remunerazione di chi ha validato le transazioni raggruppate per pagine possa essere basata anche su una parte variabile, direttamente proporzionale al valore in WTH degli scambi effettuati.

Ciò permette che al raggiungimento del numero massimo di Welthy in circolazione, il lavoro dei validatori sia comunque ricompensato.

Come avviene la retribuzione su base variabile? Ogni individuo che vuole scambiare i suoi criptoasset con altri membri della comunità può facoltativamente dichiarare, nella transazione stessa, che una parte del valore (sempre espresso in Welthy) trasferito vada a colui che valida la pagina entro cui è inserita la transazione.

Partendo dal presupposto che i validatori, in questa fase 3, non sono obbligati a validare tutti i blocchi (ricordiamo, siamo in una logica dove il governo delle regole è condiviso – come

nel mondo open source – e non vi può essere nessuna autorità centrale che obbliga qualcuno a fare il lavoro di Trent), per avere la ragionevole certezza che le proprie transazioni siano validate in tempi accettabili, è opportuno contribuire con un ulteriore incentivo sotto forma di mancia (o, se preferite, possiamo chiamarle "commissioni"). I soggetti che operano in Welthyland – in questa fase che abbiamo chiamato del governo condiviso e del controllo distribuito – privilegiano la validazione di pagine contenenti transazioni in Welthy di valore più alto, al fine di poter incassare, oltre al premio, anche la somma delle mance eventualmente

associate. Ne consegue che, anche quando fossero stati emessi tutti i Welthy a disposizione, l'economia degli scambi potrebbe comunque proseguire contando solo sulle commissioni.

---

34. Rimandiamo alle considerazioni esposte nel Capitolo 9 per un approfondimento che chiarisce il senso di questa affermazione.

35. Teoricamente, per attuare il suo reato di duplicazione a Mallory basterebbe detenere una quantità di energia elettrica tale da generare dei blackout temporanei nella città di Welthyland, che rallenterebbero l'operato di tutti gli altri validatori.

Che cosa sono gli asset nativi

A questo punto è opportuna una precisazione. Abbiamo sin qui detto che il valore del Welthy è arbitrariamente deciso dalla comunità, ovvero dal mercato e che, soprattutto, il Welthy è inteso come criptoasset rappresentativo di una proprietà (o meglio, di un diritto

al possesso) che è possibile scambiare. Negoziare tali diritti (che, non dimentichiamolo mai, sono al portatore) implica dare un valore ai medesimi prescindente (o prescindibile) dal valore dell'asset fisico rappresentato. Valorizzare il criptoasset (noi abbiamo deciso di farlo in unità di Welthy, ma potevamo scegliere qualsiasi altro nome di fantasia) richiede sia necessariamente verificata l'esistenza (o la sussistenza) dei seguenti requisiti di base:

1. la possibilità di creare "matematicamente" i criptoasset, ossia di depositarli sulla blockchain (il registro contabile

distribuito che concatena le transazioni verificate);

2. l'opportunità di creare un numero finito di criptoasset (per controllare l'inflazione[36]);

3. la possibilità di depositare i criptoasset solo a fronte di una prova di lavoro complicato da svolgere e facile da controllare che sia stato svolto correttamente (per dissuadere qualsiasi tentativo di contraffazione);

4. l'opportunità di decidere come modificare la difficoltà

della prova di lavoro (anche in questo caso per controllare le dinamiche economiche).

Il primo assunto è quello più importante. Il criptoasset che abbiamo utilizzato per spiegare i diversi modelli su cui si sono basate le tre fasi di Welthyland analizzate richiede che vi sia una tecnologia sottostante in grado di produrlo, limitandone la distribuzione. In altri termini si dice che l'asset deve essere "nativo".

In assenza di questa capacità che, ribadiamo, deve essere tipica della tecnologia e non dell'asset, probabilmente avrebbe avuto ben poco senso l'evoluzione descritta delle tre

fasi di Welthyland; ci si sarebbe potuto fermare alla sola fase 1, dove esiste un solo Trent e una sola Grace molto affidabili ed efficaci nella loro attività, ma altrettanto esposti al rischio di attacchi esogeni o debolezze endogene.

Il legame dell'asset nativo con il mondo degli scambi in un'economia reale

È possibile usare un sistema di controllo distribuito basato su una governance condivisa, così come lo abbiamo

descritto per la fase 3 di Welthyland, anche in assenza di un asset nativo, per gestire un'economia di scambi che avvengono nel mondo reale?

La risposta a questa domanda non è scontata né semplice. Cerchiamo dunque di capire se sia possibile legare "indissolubilmente" l'asset nativo a qualcosa che esiste all'esterno di Welthyland. L'avverbio che abbiamo usato (indissolubile) non è casuale e, nella sua estrema tassatività, conferisce il senso di ciò che stiamo per analizzare.

Se deve esistere qualcuno che appartiene al mondo esterno di Welthyland in grado di garantire la validità di quel diritto negoziato tramite lo scambio di criptoasset, perché

inventarsi un sistema basato sul consenso distribuito così complesso e oneroso, se poi la transazione più importante è quella che si compie all'esterno del sistema stesso?

Procediamo con ordine. L'asset nativo (e i sistemi che lo supportano) si rende molto utile in tutti quei casi in cui si debba aver **garanzia dell'immutabilità di una transazione di scambio** (anche di asset immateriali, come vedremo quando parleremo di "token") o della corretta esecuzione di un codice informatico che deve produrre un risultato inconfutabile (ne riparleremo più avanti, quando spiegheremo cosa sono i Distributed

Contract).

Può avere molto senso sfruttare una tecnologia che riesce a riprodurre il concetto di scarsità nel mondo digitale, per offrire prove incontrovertibili dell'avvenuta transazione di un bene fisico (pensiamo a una proprietà)[37] ma anche di un bene immateriale (come la quota di un fondo, un diritto d'autore o un brevetto). In tutti questi casi è però necessario che il valore del criptoasset possa essere tradable, ossia possa esprimere una forma di valore riconosciuto dalla comunità più ampia in cui il trading avviene[38]; in altre parole, il criptoasset deve avere un valore di mercato[39].

In senso più ampio, potremmo dire che laddove vi sia la necessità di legare a una transazione il rispetto della regola che ne governa la validità mentre la transazione stessa si compie, ovvero quando si riesce a usare un sistema come quello descritto per la fase 3 di Welthyland, in cui la validità del negozio giuridico che vi sottende è garantita da un sistema matematico che permette di creare quel rapporto di fiducia tra estranei senza la necessità di ricorrere a una terza parte (Trent o Grace, per usare sempre la metafora adottata), questo è probabilmente il caso d'uso più profittevole per una blockchain.

Nei successivi capitoli vi condurremo nell'affascinante mondo dei possibili impieghi di questa tecnologia, al fine non già di convincervi che la blockchain sia la soluzione di tutto, bensì per darvi contezza degli ambiti in cui il suo valore potrebbe rivelarsi più o meno apprezzabile.

Ma, prima di procedere in questa direzione, ci manca ancora un ultimo aspetto importante da analizzare: capire i pregi e i difetti dei tre modelli che abbiamo presentato, nonché le motivazioni che possano supportare la scelta di uno di essi. Quali sono i rischi e le opportunità che, con ciascun modello, caratterizzano la comunità di

Welthyland? Dove sono i punti di forza e quelli di debolezza? Nel seguito proveremo a sintetizzare in un'analisi SWOT tutti questi aspetti, al fine di consentirvi una confrontabilità dei diversi modelli che classificheremo in due macrocategorie:

1. **Centralized Ledger**, ossia l'architettura definita per la fase 1.
2. **Distributed Ledger**, ossia le architetture definite per le fasi 2 e 3.

---

36. Se non ci fosse la prova di lavoro complicata da produrre, ognuno tenderebbe a depositare criptoasset all'infinito,

inflazionando in pochi istanti l'economia di Welthyland.

37. Vediamo per esempio un'applicazione di notarizzazione, che garantisce l'immutabilità di una marcatura temporale (timestamp) applicata a qualsiasi evento tracciabile.

38. I casi d'esempio più esaustivi sono rappresentati dalle blockchain basate su Distributed Ledger permissionless, come quella dei Bitcoin o quella di Ethereum, che vede nell'Ether il proprio criptoasset.

39. Volutamente non ci si sofferma in questo libro (giacché non rientra nel suo scopo) sulla disamina delle opportunità e dei vincoli legati alla regolamentazione di questo mercato che, peraltro, alla data in cui scriviamo, non è ancora regolamentato in Europa.

8

Centralized Ledger vs Distributed Ledger

Avrete di certo colto come la macrocategorizzazione che vi abbiamo proposto preveda due tipologie di ledger e non tre, ossia tanti quanti erano i modelli adottati nelle fasi di

Welthyland.

La Figura 8.1 può essere d'aiuto per meglio comprendere le ragioni di questa scelta. Volutamente abbiamo raggruppato sotto la definizione di "Distributed Ledger" sia il modello impiegato nel periodo del governo centralizzato e dei controlli distribuiti sia quello adottato nel periodo del governo condiviso e del controllo distribuito. In ambedue i casi, contrariamente al primo, il ledger è condiviso con una pluralità di membri che assumono il ruolo "distribuito" di Trent e di Grace.

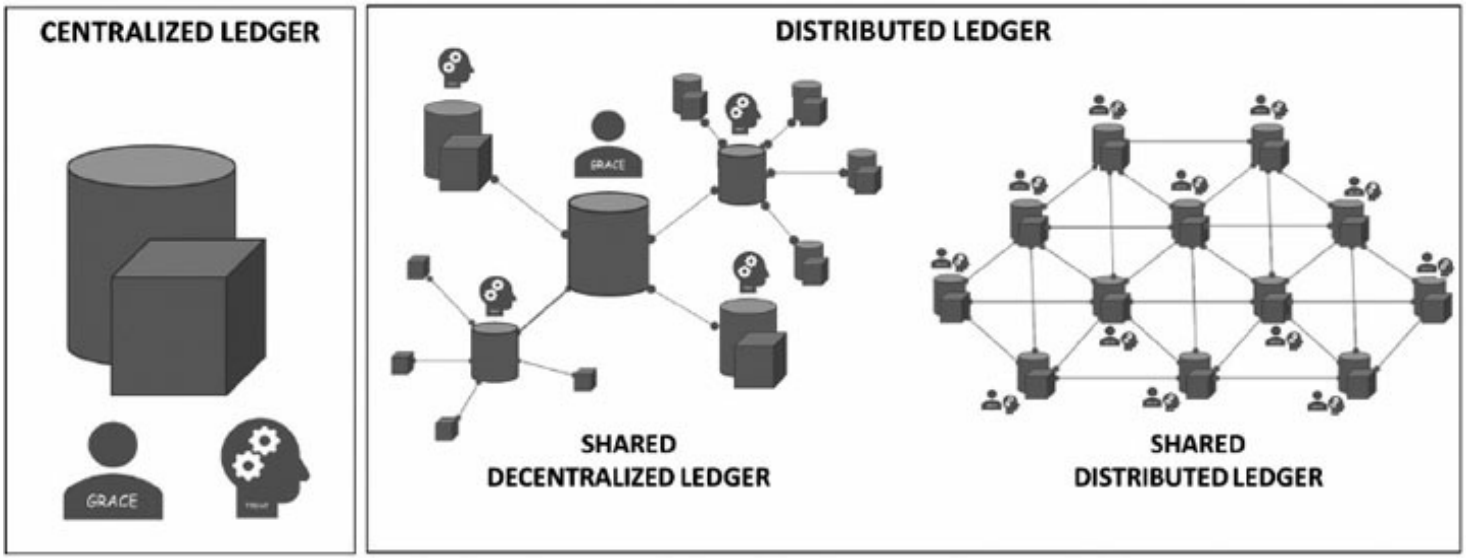

Figura 8.1 – Confronto fra Centralized Ledger e Distributed Ledger.

Più propriamente, diremo che questa configurazione è quella che giustifica l'adozione di una blockchain, cui, sotto il profilo meramente tecnologico, sottende ciò che viene chiamato con il nome di "DLT", Distributed Ledger Technology (Figura 8.1).

Procediamo ora con l'analisi SWOT per ciascun modello, usando ancora la

metafora di Welthyland.

L’analisi SWOT per la fase 1 (Centralized Ledger)

I punti di forza nella fase 1 (modello del governo centralizzato)

In questa fase Welthyland sa che può contare sull’efficacia di validazione di Trent; la fiducia che Welthyland ripone in lui e l’aver ben compreso che la sua retribuzione, così come la sua capacità, sono valutate da Grace sulla base di

regole note e condivise con la comunità, permettono all'intero sistema economico di scambi un buon livello di efficienza.

I punti di debolezza nella fase 1 (periodo del governo centralizzato)

In questa fase Welthyland sa perfettamente che Trent, con il passare del tempo o con l'aumentare della frequenza degli scambi, potrebbe non garantire più un livello di efficienza accettabile. Fintanto che Trent non sarà

sostituito da un Trent più giovane o fino a che Grace non decide di modificare le politiche retributive del nostro vecchio saggio[40], l'economia di Welthyland non è al sicuro.

Le opportunità nella fase 1 (periodo del governo centralizzato)

I membri della comunità di Welthyland sanno che, in questa fase, possono contribuire in modo indiretto, ma decisivo, al benessere della loro economia. Se dovessero ritenere

realmente utili (se non necessari) taluni miglioramenti al processo di validazione, potrebbero analizzare insieme a Grace nuovi sistemi e, nel successivo passaggio consultivo, votare per il cambiamento delle regole. La loro partecipazione al processo di miglioramento, però, non avviene ancora in forma diretta e ciò potrebbe non essere un danno (entro certi limiti) perché non è detto che, laddove anche solo pensassero di contribuire a migliorare il lavoro di Trent sostituendosi a esso, ne sarebbero realmente capaci.

I rischi nella fase 1 (periodo del governo centralizzato)

In questa fase a Welthyland possono accadere diverse situazioni molto spiacevoli, al verificarsi delle quali l'intera comunità non avrebbe più la garanzia che i propri scambi di valore fossero certi, sicuri e immutabili.

Proviamo ad elencare alcuni possibili rischi cui il modello adottato per gestire il trasferimento dei Welthy nel periodo del governo centralizzato è esposto:

1. **Mallory** attacca Trent

impedendogli di fare bene il suo lavoro, per esempio contaminandolo con un virus che lo fa ammalare e che produrrà un calo di efficienza nel suo operato.

2. **Mallory** attacca Trent mettendolo definitivamente in condizione di non poter operare, per esempio rompendo l'orologio su cui Trent si basa per annotare le transazioni e chiudere le pagine del libro contabile.

3. **Mallory** attacca Trent costringendolo ad alterare la storia delle transazioni

annotate sul registro delle transazioni, per esempio minacciandolo fisicamente.

4. **Mallory** corrompe Trent costringendolo ad alterare la storia delle transazioni annotate sul registro delle transazioni.

5. **Mallory** conosce alcune debolezze di Trent e può tenerlo sotto scacco, obbligandolo a fare ciò che non vorrebbe.

6. **Mallory** corrompe Grace e fa in modo che giudichi l'operato di Trent non più efficace, al fine di aver un

pretesto per intervenire (a danno di Trent e della comunità tutta) nella politica retributiva di Trent (lo scopo è distruggere Trent e l'economia di scambi basata sul modello di fase 1).

7. **Trent** si disamora del suo lavoro e, nonostante gli venga riconosciuta la possibilità (da Grace) di un aumento delle ricompense che sa che potrebbe ancora meritare (perché non è stanco o ammalato e ha ancora molta energia), finisce con il degradare il suo operato,

incrinando il rapporto di fiducia con gli abitanti di Welthyland.

Volendo categorizzare i rischi, potremmo dire che nella fase 1 di Welthyland si ha la classificazione presente in Tabella 8.1.

Tipologia di rischio	Rischio	Possibile rimedio	Note
Rischio tecnico	1	Replicare Trent	Replicare non significa distribuire
	2	Avere un sistema di back-up	Back-up a caldo
	3	Nessuno	Se Trent fosse replicato, anche l'azione eseguita sotto minaccia lo sarebbe
Rischio reputazionale	4	Intervento di Grace (non immediato)	Grace per intervenire ha bisogno di mettere a conoscenza tutti e fare un passaggio consultivo
	5	Intervento di Grace (non immediato e potenzialmente meno efficace)	Grace per intervenire ha bisogno di mettere a conoscenza tutti e fare un passaggio consultivo; potenzialmente Grace sarebbe esposta al medesimo rischio laddove Mallory scoprisse che le debolezze di Trent erano già note a Grace
Rischio di sistema	6	Nessuno	
	7	Nessuno	

Tabella 8.1 – Classificazione dei rischi nel

modello del governo centralizzato.

L’analisi SWOT per la fase 2 (Shared Decentralized Ledger)

I punti di forza nella fase 2 (modello del governo centralizzato e dei controlli distribuiti)

In questa fase, Welthyland sa che può contare sull’efficacia di validazione dei Trent, ossia di soggetti che Grace ha debitamente preselezionato. La fiducia

che Welthyland ripone nei Trent e l'aver ben compreso che le loro capacità sono valutate da Grace sulla base di regole note e condivise con la comunità permettono all'intero sistema economico di scambi un buon livello di efficienza.

I punti di debolezza nella fase 2 (modello del governo centralizzato e dei controlli distribuiti)

In questa fase Welthyland sa

perfettamente che Grace è esposta alla politica della stessa comunità e che il livello di fiducia in essa riposto potrebbe cambiare a fronte di eventi sociali (periodi di crisi, rivolte *et similia*) o naturali (carestia, terremoti, siccità, pandemie). In tutti questi casi l'espressione democratica dei cittadini di Welthyland manifestata tramite l'elezione di Grace, nonché l'accettazione delle regole che erano state condivise prima dell'elezione, sono drasticamente esposte. Fintanto che Grace non riprenderà democraticamente il pieno controllo di Welthyland, l'economia di Welthyland non è al sicuro.

Le opportunità nella fase 2 (modello del governo centralizzato e dei controlli distribuiti)

In modo del tutto simile alla fase 1, i membri della comunità di Welthyland sanno che, con questo modello, possono contribuire in modo indiretto, ma decisivo, al benessere della loro economia. Se ritenessero davvero utili alcuni miglioramenti al processo di validazione, potrebbero analizzare insieme a Grace nuovi sistemi e, nel

successivo passaggio consultivo, votare per il cambiamento delle regole. La loro partecipazione al processo di miglioramento, come per la fase 1, non avviene ancora in forma diretta e ciò potrebbe non essere, anche in questo caso, un danno (entro certi limiti) perché non è detto che, laddove anche solo pensassero di contribuire a migliorare il lavoro dei Trent sostituendosi a essi, ne sarebbero realmente capaci.

I rischi nella fase 2 (modello del governo centralizzato e dei

controlli distribuiti)

In questa fase a Welthyland possono accadere diverse situazioni sgradite, al verificarsi delle quali l'intera comunità non avrebbe più la garanzia che i propri scambi di valore fossero certi, sicuri e immutabili.

Proviamo a elencare alcuni possibili rischi cui il modello adottato per gestire il trasferimento dei Welthy in questo periodo è esposto:

1. **Mallory** corrompe la maggioranza dei Trent obbligando un consenso distribuito che prevale su quello dei Trent onesti e

consente di alterare la storia delle transazioni annotate sul registro delle transazioni.

2. **Mallory** tramite Grace diffonde un virus pandemico che fa ammalare tutti i Trent al fine di conseguire con maggiore facilità lo scopo criminoso di cui al punto precedente (i Trent che ancora sopravvivono saranno pochi rispetto alla normalità e, verosimilmente, più deboli).

3. **Mallory** corrompe Grace e fa in modo che giudichi l'operato dei Trent non più

efficace al fine di aver un pretesto per sostituirli rimpiazzandoli con suoi sodali; lo scopo è eliminare tutti i Trent precedentemente individuati da Grace quando poteva dirsi onesta e godeva della fiducia degli abitanti di Welthyland; la sostituzione dei Trent passerà come una scelta di Grace, sempre in ordine all'antico mandato ricevuto dalla collettività.

4. **Mallory** discredita Grace diffondendo presso gli abitanti di Welthyland false verità e crea i presupposti per

destabilizzare il sistema di governo; la fase di discontinuità che si viene a creare sarà tale da poter consentire una facile presa del potere (Grace verrà destituita) ad appannaggio degli scopi criminosi di Mallory.

Volendo categorizzare i rischi, potremmo dire che nella fase 2 di Welthyland si ha la classificazione presentata in Tabella 8.2.

Tipologia di rischio	Rischio	Possibile rimedio	Note
Rischio reputazionale	1	Intervento di Grace (non immediato)	Grace per intervenire potrebbe non aver bisogno di mettere a conoscenza tutti facendo obbligatoriamente un passaggio consultivo
Rischio reputazionale/ tecnico	2	Intervento di Grace (non immediato)	Grace deve prima comprendere di essere il veicolo del virus, quindi deve debellarlo e, successivamente, provvedere alla sostituzione dei Trent ammalati individuandone di nuovi
Rischio di sistema	3	I membri di Welthyland potrebbero aver inserito una clausola nel mandato di Grace che la obbliga a giustificare le motivazioni di qualsiasi sostituzione di Trent, in tal modo avrebbero contezza degli eccessivi avvicendamenti dei Trent e potrebbero accorgersi di un comportamento anomalo di Grace	Il rischio che Welthyland corre è molto grave e potrebbe non avere via d'uscita
	4	Nessuno	

Tabella 8.2 – Classificazione dei rischi nel modello del governo centralizzato e dei controlli distribuiti.

L'analisi SWOT per la fase 3 (Shared

Distributed Ledger)

I punti di forza nella fase 3 (modello del governo condiviso e del controllo distribuito)

In questa fase Welthyland decide di adottare una tecnologia che abilita abitanti diversi, fra di loro sconosciuti, a verificare il succedersi di transazioni in Welthy registrate su un libro mastro distribuito ("Distributed Ledger") e raggruppate in concatenazione all'interno di "blocchi". Il Distributed Ledger viene acceduto dai partecipanti che operano sulla rete (tramite dei

“nodi”) mettendo a disposizione risorse di calcolo, mediante cui si ottempera alla validazione delle transazioni, evitando così il ricorso a un intermediario terzo (Trent o, se preferite, la coppia Trent & Grace). Tali partecipanti assumono il ruolo di validatori. Durante questo processo vengono “coniate” nuove unità di Welthy come sistema di remunerazione che ripaga – almeno in parte – il costo sostenuto dai validatori (risorse di calcolo, energetiche ecc.). Il modello d’incentivazione assicura che questi ultimi vengano remunerati per il loro lavoro di approvazione solo laddove il compito sia stato svolto correttamente (verificato dagli altri partecipanti),

rendendo antieconomico qualsiasi tentativo di alterazione surrettizia dei blocchi precedentemente validati.

Tracciabilità (da tutti i partecipanti al sistema), immutabilità e sicurezza sono quindi le caratteristiche principali che connotano il modello adottato da Welthyland nella fase 3. Più in generale possiamo dire che Welthyland ha individuato un sistema che permette di stabilire relazioni fiduciarie tra soggetti che non si conoscono, riducendo drasticamente le vulnerabilità (tipiche delle fasi precedenti) che consentivano a Mallory di perpetrare i suoi attacchi: non ci sono più né Grace né Trent, in quanto unici e riconoscibili, bensì vi è

una pluralità di soggetti che, condividendo delle regole note, non necessita di conoscersi e può svolgere in modo distribuito i compiti che erano assegnati a persone definite nei modelli di fase 1 e 2.

I punti di debolezza nella fase 3 (modello del governo condiviso e del controllo distribuito)

In questa fase Welthyland deve sapere

che la propria economia di scambi basati sui Welthy presenta alcune debolezze essenzialmente connaturate all'impiego di una tecnologia come la blockchain descritta.

Esiste dapprima un grave problema di privacy. Tutte le transazioni avvengono in chiaro e per ciascuna di esse rimane una traccia immutabile della loro storia[41].

Per come avviene il processo di scambio e validazione che abbiamo descritto sulla blockchain adottata dalla nostra immaginaria società, i Welthy trasferiti non possono essere mai stornati; ciò, in alcuni casi, potrebbe rappresentare un problema.

Il fatto che ogni membro della comunità possa assurgere al ruolo di validatore implica una responsabilità in capo al singolo individuo che, mai come in questo caso, comprende di essere un "con-dividuo". Qualsiasi debolezza del singolo rischia di essere la debolezza dell'intera comunità. Sebbene il sistema sotteso alla prova di lavoro che ognuno deve presentare per validare i blocchi di transazioni (e per ottenere le ricompense) sia matematicamente sicuro, una possibile coalizione di individui validatori che riuscisse a possedere una potenza di calcolo pari al 51% delle risorse in campo potrebbe teoricamente riproporre un modello

“Trent-centrico”. Infine (ma non ultima per importanza) la distribuzione dei controlli verificata sulla risoluzione di un enigma crittografico che richiede consumi energetici elevati espone la comunità a un rischio di inefficienza prestazionale che potrebbe allungare di molto il processo di validazione, rispetto alle fasi 1 e 2.

Le opportunità nella fase 3 (modello del governo condiviso e del controllo

distribuito)

Le opportunità presenti in questa fase saranno specificamente trattate nella Parte IV di questo libro (alla quale vi rimandiamo), laddove parleremo di strategie che possono essere indirizzate da una blockchain come quella su cui Welthyland ha deciso di basarsi.

I rischi nella fase 3 (modello del governo condiviso e del controllo distribuito)

Anche per quanto concerne i rischi cui si espone Welthyland nell'adozione di una soluzione come quella descritta per questa terza fase, faremo nella Parte II del libro una disamina volta a evincere le principali criticità.

---

40. È utile sottolineare che Grace potrebbe cambiare le regole solo a fronte di un nuovo passaggio consultivo con la popolazione; inoltre, questa modalità potrebbe non garantire appieno il conseguimento degli obiettivi prefissi, laddove Trent non ce la facesse comunque, nonostante un aumento del suo stipendio.

41. Questo significa che vi sono problemi anche legati al diritto di oblio.

PARTE II
ALL'INTERNO DELLA BLOCKCHAIN

La consapevolezza è la tua stessa natura:
puoi dimenticarla, ma non puoi perderla.
Non può essere rubata. È il tuo stesso centro.

Osho Rajneesh

9

La Blockchain con la “B” maiuscola

Dopo aver descritto i fondamentali della blockchain tramite la metafora di Welthyland e dei suoi tre modelli su cui si sono sviluppate le regole del consenso e della fiducia che ogni abitante adotta per garantire la bontà degli scambi di Welthy, siamo giunti al

punto in cui, forti della consapevolezza fin qui acquisita, possiamo avviarci insieme in un percorso di conoscenza finalizzato a comprendere come funziona la più famosa delle blockchain[42] attualmente operative: la Blockchain dei Bitcoin.

In questo capitolo vedremo nel dettaglio come avviene una transazione in Bitcoin, al fine di potervi consentire la migliore comprensione di ciò che è possibile realizzare su un'infrastruttura Distributed Ledger. In tal senso, ci concentreremo sulla tecnologia alla base dei Bitcoin, non già volendola scindere dalla criptovaluta, bensì spiegando come la presenza di un asset nativo sia

funzionalmente necessaria ed essenzialmente utile al fine di consentire un reale beneficio alle applicazioni che su di essa potranno essere implementate.

Che cos'è una Blockchain

Possiamo definire la Blockchain – in modo sommario ma sufficientemente valido per poterci permettere di proseguire nel nostro percorso – come una tecnologia in cui esiste un database di transazioni condiviso tra più nodi di una rete, validato dalla rete stessa e strutturato a blocchi (una catena di blocchi che contengono più transazioni).

Le principali caratteristiche del database sono:

- tracciabilità da tutti i partecipanti alla rete;
- immutabilità e sicurezza attraverso sistemi crittografici.

L'utilità della Blockchain

Vi sono ambiti che possono trarre un reale vantaggio dall'adozione di soluzioni che si basano su Blockchain, altri per i quali può essere ininfluente, altri ancora in cui provocherebbe impatti negativi. Volendo sintetizzare,

mostriamo quali sono le principali ragioni che dovrebbero supportare la scelta di sviluppare un progetto su Blockchain, ossia quali dovrebbero essere le condizioni al verificarsi delle quali può essere utile adottare una soluzione basata su Blockchain:

- immutabilità delle transazioni;
- trasparenza;
- numerosità ed eterogeneità degli attori;
- sfiducia fra i partecipanti.

Per capire questa nuova tecnologia e valutarne i reali benefici occorre innanzitutto non confonderla con i Bitcoin, chiarendo le caratteristiche che

la rendono unica e comprendendo quali sono le effettive opportunità.

Non confondiamo i Bitcoin con la Blockchain, ma contemperiamoli!

È opinione piuttosto diffusa quella che vorrebbe considerare la Blockchain disgiunta dai Bitcoin, pretendendo di dimostrare come la criptovaluta non sia indispensabile. Noi, invece, riteniamo necessario considerare la presenza di un asset nativo e l'impiego del medesimo a

supporto di un sistema che, senza di esso, non riuscirebbe a riprodurre il concetto di scarsità nel mondo digitale. È proprio grazie alla presenza di un criptoasset "matematicamente scarso" che una blockchain[43] riesce a offrire il meglio di sé, ossia rende possibile garantire l'incontestabilità e l'immutabilità delle transazioni e dei dati in un ambiente decentralizzato dove la fiducia è provata crittograficamente, il consenso è un processo distribuito fra più soggetti e il governo delle regole è condiviso fra più attori.

Alcune definizioni per

descrivere la Blockchain

Prima di addentrarci in una puntuale descrizione del funzionamento della Blockchain è utile condividere una tassonomia che ci permetta di attribuire ai termini che useremo un significato coerente. Per agevolarvi nella comprensione useremo ancora l'analogia con Welthyland che ci ha accompagnato nella Parte I del libro, mappando opportunamente, sull'ontologia della Blockchain che andiamo a proporvi, i concetti già espressi in metafora. Nella Tabella 9.1 riportiamo la mappatura sulle tre fasi di

Welthyland delle definizioni che esporremo nei successivi capitoli. Le definizioni non sono organizzate alfabeticamente; l'ordine adottato rispecchia la logica con cui spiegheremo – in sequenza – il loro significato.

Definizioni Blockchain	**Metafora Welthyland – Fasi**
Criptoasset	In tutte le tre fasi
Btc	In tutte le tre fasi
Nodo	In tutte le tre fasi
Transazione	In tutte le tre fasi
Transazione verificata	In tutte le tre fasi
Transazione validata	In tutte le tre fasi
Transazione confermata	Solo fase 3 e fase 2
Blocco	In tutte le tre fasi

Ledger	In tutte le tre fasi
Hash	Solo fase 3 (in fase 1 e 2 è comunque possibile traslarne il significato)
Target	Solo fase 3
Difficoltà	Solo fase 3
Miner	Solo fase 3 (in fase 1 e 2 è comunque possibile traslarne il significato)
Mining	Solo fase 3 (in fase 1 e 2 è comunque possibile traslarne il significato)
PoW (Proof-Of-Work)	Solo fase 3
Nonce	Solo fase 3
Reward	Solo fase 3 (in fase 1 e 2 assumono il significato descritto per “deposito”)
Mance (o commissioni)	In tutte le tre fasi
Protocollo	In tutte le tre fasi
Network	Solo fase 3 e fase 2
Wallet	Solo fase 3 (in fase 1 e 2 è comunque possibile traslarne il significato)
Firma digitale	Solo fase 3 (in fase 1 e 2 è comunque

	possibile traslarne il significato)
Chiave privata	Non presente
Chiave pubblica	Non presente
Address	In tutte le tre fasi

Tabella 9.1 – Perimetro di mappatura della Blockchain sulla metafora di Welthyland.

Veniamo dunque a descrivere le definizioni che useremo per spiegare la Blockchain.

Criptoasset

Il criptoasset è l'asset nativo che nella Blockchain è costituito dai Bitcoin. Nella metafora di Welthyland coincide con i Welthy.

BTC

È l'abbreviazione di Bitcoin. Nella metafora di Welthyland è chiamato WTH (abbreviazione di Welthy).

Nodo

I partecipanti alla Blockchain vengono chiamati "nodi"; sono costituiti fisicamente da server mediante i quali vengono gestite le transazioni in criptoasset. Per la metafora di Welthyland vedere la Tabella 9.2.

Metafora	Welthyland
Fase 1	Trent

Fase 2	La pluralità di Trent, Grace
Fase 3	I membri di Welthyland

Tabella 9.2 – Mappatura di nodo sulla metafora di Welthyland.

Transazione

Uno scambio di criptoasset tra due o più nodi si chiama genericamente transazione. Nella metafora di Welthyland è rappresentata dallo scambio di Welthy tra i membri della comunità (per esempio fra Alice e Bob).

Transazione verificata

È la singola transazione verificata dai

nodi partecipanti. Per la metafora di Welthyland guardate la Tabella 9.3.

Metafora	Welthyland
Fase 1	Transazione verificata da Trent prima della contabilizzazione
Fase 2	Transazione verificata dai Trent prima della contabilizzazione
Fase 3	Transazione verificata dai membri di Welthyland prima di essere inclusa in una pagina validata

Tabella 9.3 – Mappatura di transazione verificata sulla metafora di Welthyland.

Transazione validata

È una transazione verificata che si trova in un blocco validato. Per la metafora di Welthyland vedere la Tabella 9.4.

Metafora	Welthyland
Fase 1	Transazione contabilizzata da Trent
Fase 2	Transazione contabilizzata dai Trent in una pagina in attesa della validazione (a fronte del raggiungimento di un consenso distribuito tra la maggioranza dei Trent)
Fase 3	Transazione verificata inclusa in una pagina validata (almeno una volta) dai membri di Welthyland validatori

Tabella 9.4 – Mappatura di transazione validata sulla metafora di Welthyland.

Transazione confermata

È una transazione verificata che si trova in un blocco validato distante dall'ultimo blocco validato di almeno 5 posizioni. Nel sistema Bitcoin, poiché mediamente ogni 10 minuti viene

validato un blocco e aggiunto alla catena, si ha una transazione confermata ogni 60 minuti. Per la metafora di Welthyland vedere la Tabella 9.5.

Metafora	Welthyland
Fase 1	Non esiste
Fase 2	Transazione contabilizzata dai Trent in una pagina validata dalla maggioranza dei Trent
Fase 3	Transazione verificata inclusa in una pagina validata almeno 6 volte dai membri di Welthyland validatori

Tabella 9.5 – Mappatura di transazione confermata sulla metafora di Welthyland.

Blocco

Il blocco è un raggruppamento di

transazioni verificate. È un'unita di cui si compone la Blockchain che contiene tutte le transazioni verificate durante il periodo di generazione del blocco stesso; mediamente ogni 10 minuti viene generato un nuovo blocco e aggiunto in modo cronologico alla catena di blocchi. Nella metafora Welthyland è rappresentato dalla quella che abbiamo chiamato "pagina contabile".

Ledger

È il registro pubblico distribuito (Distributed Ledger) nel quale vengono "annotate" con la massima trasparenza tutte le transazioni effettuate in modo

ordinato e sequenziale. Il ledger è costituito da una serie di blocchi che sono tra loro incatenati mediante una funzione crittografica e l'uso di Hash. La tecnologia che gestisce il ledger si chiama "Distributed Ledger Technology" (DLT) ed è utilizzata, spesso impropriamente, per indicare una blockchain. Nella metafora di Welthyland coincide con il libro mastro.

Hash (o funzione di Hash)

La funzione di Hash è un sistema matematico che consente di convertire

un messaggio di lunghezza arbitraria in un messaggio in codice alfanumerico di lunghezza fissa (o prefissata) chiamata Digest o impronta digitale. Per la metafora di Welthyland vedere la Tabella 9.6.

Metafora	Welthyland
Fase 1	Traslando il concetto sotto il profilo meramente funzionale, il calcolo dell'Hash potrebbe essere assimilato ai calcoli che Trent deve eseguire alla fine dell'intervallo di tempo (10 minuti) sulle transazioni che si sono compiute, secondo le regole istruite da Grace
Fase 2	Traslando il concetto sotto il profilo meramente funzionale, il calcolo dell'Hash potrebbe essere assimilato ai calcoli che ciascun Trent deve eseguire alla fine dell'intervallo di tempo (10 minuti) sulle transazioni che si sono compiute, secondo le regole istruite da Grace

Fase 3	Rappresenta l'anagramma.

Tabella 9.6 – Mappatura di funzione di Hash sulla metafora di Welthyland.

Target

Il target è un numero estremamente grande (a 256 bit) il cui valore si modifica in base al tempo effettivo e teorico necessario per validare 2.016 blocchi. Più il target è piccolo e più è difficile ricercare una soluzione che lo possa soddisfare. Per la metafora di Welthyland vedere la Tabella 9.7.

Metafora	Welthyland
Fase 1	Non presente perché non necessario

Fase 2	Non presente perché non necessario
Fase 3	Rappresenta come deve essere creato l'anagramma di senso compiuto che i membri validatori devono risolvere in competizione fra loro (per esempio deve contenere 5 parole di lunghezza non superiore a 4 lettere)

Tabella 9.7 – Mappatura di target sulla metafora di Welthyland.

Difficoltà

Rappresenta la misura di quanto sia complicato trovare un Hash al di sotto di un certo target. Nella Blockchain dei Bitcoin non può essere inferiore a 1 e viene aggiustata ogni 2.016 blocchi, ossia mediamente ogni 12 giorni; è un valore inversamente correlato al target e

positivamente correlato all'Hash rate. Per la metafora di Welthyland vedere la Tabella 9.8.

Metafora	Welthyland
Fase 1	Non presente perché non necessario
Fase 2	Non presente perché non necessario
Fase 3	Rappresenta il livello di difficoltà – deciso dalla comunità di Welthyland – dell'anagramma che i membri validatori devono risolvere in competizione fra loro

Tabella 9.8 – Mappatura di difficoltà sulla metafora di Welthyland.

Miner (o minatore)

Nella Blockchain un miner è un nodo validatore dei blocchi. Per la metafora

di Welthyland vedere la Tabella 9.9.

Metafora	Welthyland
Fase 1	Il singolo Trent
Fase 2	La pluralità di Trent
Fase 3	I membri di Welthyland validatori

Tabella 9.9 – Mappatura di miner sulla metafora di Welthyland.

Mining

Nella Blockchain il mining è il processo con cui si validano e registrano le transazioni. Per la metafora di Welthyland vedere la Tabella 9.10.

Metafora	Welthyland

Fase 1	È l'attività svolta da Trent di validazione del libro mastro
Fase 2	È l'attività svolta dai Trent di validazione del libro mastro distribuito
Fase 3	È l'attività svolta dai membri di Welthyland validatori

Tabella 9.10 – Mappatura di mining sulla metafora di Welthyland.

PoW, Proof-of-Work (o prova di lavoro)

Nella Blockchain dei Bitcoin è la prova che consente ai miner di dimostrare a tutti gli altri nodi la validazione del blocco e che permette loro di ottenere la ricompensa (più le eventuali mance). Per la metafora di Welthyland vedere la

Tabella 9.11.

Metafora	Welthyland
Fase 1	Non presente
Fase 2	Non presente
Fase 3	Soluzione dell'anagramma

Tabella 9.11 – Mappatura di Proof-of-Work sulla metafora di Welthyland.

Nonce

È una stringa casuale di dati che viene utilizzata nel processo di hashing di un blocco; viene utilizzato un nonce diverso per ogni tentativo di hashing, al fine di soddisfare il target richiesto nel processo di mining di un blocco. Per la

metafora di Welthyland vedere la Tabella 9.12.

Metafora	Welthyland
Fase 1	Non presente
Fase 2	Non presente
Fase 3	Tentativi di soluzione dell'anagramma messi in atto dai membri di Welthyland per validare le pagine

Tabella 9.12 – Mappatura di nonce sulla metafora di Welthyland.

Reward (o ricompensa)

Nella Blockchain costituisce la remunerazione dei miner in criptoasset.

Per la metafora di Welthyland vedere la Tabella 9.13.

Metafora	Welthyland
Fase 1	Deposito di Welthy iniziale di Alice, Bob ecc.
Fase 2	Deposito di Welthy iniziale di Alice, Bob ecc.
Fase 3	Ricompensa/deposito in Welthy dei membri di Welthyland validatori che hanno presentato la PoW

Tabella 9.13 – Mappatura di reward sulla metafora di Welthyland.

Mance (o commissioni)

Mance (o commissioni) liberamente

incluse nelle transazioni su iniziativa dei singoli che i miner possono incassare a lavoro di validazione compiuto (servono da incentivo per i miner). Per la metafora di Welthyland vedere la Tabella 9.14.

Metafora	Welthyland
Fase 1	Quota parte variabile della retribuzione di Trent decisa da Grace
Fase 2	Quota parte variabile della retribuzione dei Trent decisa da Grace
Fase 3	Ulteriore ricompensa in Welthy dei membri di Welthyland validatori che hanno presentato la PoW

Tabella 9.14 – Mappatura di mance sulla metafora di Welthyland.

Protocollo

Nella Blockchain il protocollo rappresenta l'insieme di regole condivise da tutti i nodi che, essenzialmente, definiscono:

- la dimensione dei blocchi;
- come deve essere raggiunto il consenso distribuito;
- la politica di incentivazione e remunerazione dei miner;
- la variazione dei livelli di difficoltà.

Per la metafora di Welthyland vedere la Tabella 9.15.

Metafora	Welthyland
Fase 1	Regole decise da Grace a posteriori della sua elezione voluta degli abitanti di Welthyland
Fase 2	Regole decise da Grace a posteriori della sua elezione voluta degli abitanti di Welthyland
Fase 3	Regole condivise – e accettate – tra tutti i membri di Welthyland

Tabella 9.15 – Mappatura di protocollo sulla metafora di Welthyland.

Network

Il sistema Bitcoin della Blockchain è organizzato in nodi secondo una rete distribuita, decentralizzata e paritaria; il network Bitcoin è costruito dunque su sistema di tipo P2P (Peer-to-Peer). Per

la metafora di Welthyland vedere la Tabella 9.16.

Metafora	Welthyland
Fase 1	Non presente
Fase 2	Presente, ma solo nella configurazione “Shared Decentralized Ledger” non P2P
Fase 3	Presente nella configurazione “Shared Distributed Ledger” P2P

Tabella 9.16 – Mappatura di network sulla metafora di Welthyland.

Wallet

Portafoglio elettronico che memorizza tutte le credenziali per accedere, spendere e trasferire criptoasset. Per la metafora di Welthyland vedere la

Tabella 9.17.

Metafora	Welthyland
Fase 1	Traslando il concetto sotto il profilo meramente funzionale, è assimilabile alla cassaforte gestita da Trent nella quale viene custodito il libro mastro
Fase 2	Traslando il concetto sotto il profilo meramente funzionale, è assimilabile alle copie del libro mastro accedute in sicurezza dalla pluralità di Trent
Fase 3	È lo strumento con cui tutti i membri di Welthyland possono scambiarsi Welthy

Tabella 9.17 – Mappatura di wallet sulla metafora di Welthyland

Firma digitale

Si tratta di un processo crittografico basato su chiavi asimmetriche che,

insieme alla funzione di Hash, permette di provare che una transazione in Bitcoin sia generata da chi realmente è in grado di accedere al proprio wallet. Per la metafora di Welthyland vedere la Tabella 9.18.

Metafora	Welthyland
Fase 1	Traslando il concetto sotto il profilo meramente funzionale, è assimilabile alla firma che Trent appone sul libro mastro ad ogni transazione
Fase 2	Traslando il concetto sotto il profilo meramente funzionale, è assimilabile alla firma che la pluralità di Trent appone sulle copie del libro mastro accedute in sicurezza a ogni transazione
Fase 3	È lo strumento mediante il quale tutti i membri di Welthyland possono verificare le transazioni che poi si inseriranno nel successivo blocco in attesa di validazione

Tabella 9.18 – Mappatura di firma digitale sulla metafora di Welthyland.

Chiave privata

È una chiave crittografica utilizzata in un sistema di crittografia asimmetrica e deve essere custodita gelosamente; nel sistema Bitcoin la chiave privata si compone di un codice alfanumerico associato a ogni wallet. Nella metafora di Welthyland non esiste la chiave privata (in nessuna fase).

Chiave pubblica

È una chiave crittografica utilizzata in un sistema di crittografia asimmetrica che

può essere scambiata anche su un canale non sicuro; nel sistema Bitcoin la chiave pubblica è rappresentata dall'Address. Nella metafora di Welthyland non esiste la chiave pubblica (in nessuna fase).

Address

Coincide con la chiave pubblica di un wallet ed è formata da una stringa di caratteri alfanumerici utilizzata per ricevere o inviare le transazioni. Per la metafora di Welthyland, traslando il concetto sotto il profilo meramente funzionale, è assimilabile a ciò che abbiamo chiamato "generalità" in tutte le fasi.

42. Ricordiamo sempre di prestare attenzione allo stile (maiuscolo/minuscolo) dell'iniziale del termine "blockchain" che abbiamo spiegato all'inizio del libro: con il termine "Blockchain" (quando l'iniziale è maiuscola) ci si riferisce alla tecnologia che supporta i Bitcoin, mentre con il termine "blockchain" (con l'iniziale minuscola) si intende l'architettura tecnologica posta alla base di altri sistemi dove il criptoasset non è necessariamente il Bitcoin.

43. In questo caso l'iniziale è volutamente in minuscolo, con ciò significando che possono esistere altre architetture basate su Distributed Ledger alternative a quella che sottende ai Bitcoin, nelle quali è presente un asset nativo.

10

Il processo che descrive la Blockchain

Chiariti i termini che adotteremo nei successivi paragrafi e il loro significato, andiamo ora a descrivere la Blockchain analizzando il ciclo di vita di una transazione che su di essa si compie.

Nella Figura 10.1 è riportato lo schema che adotteremo.

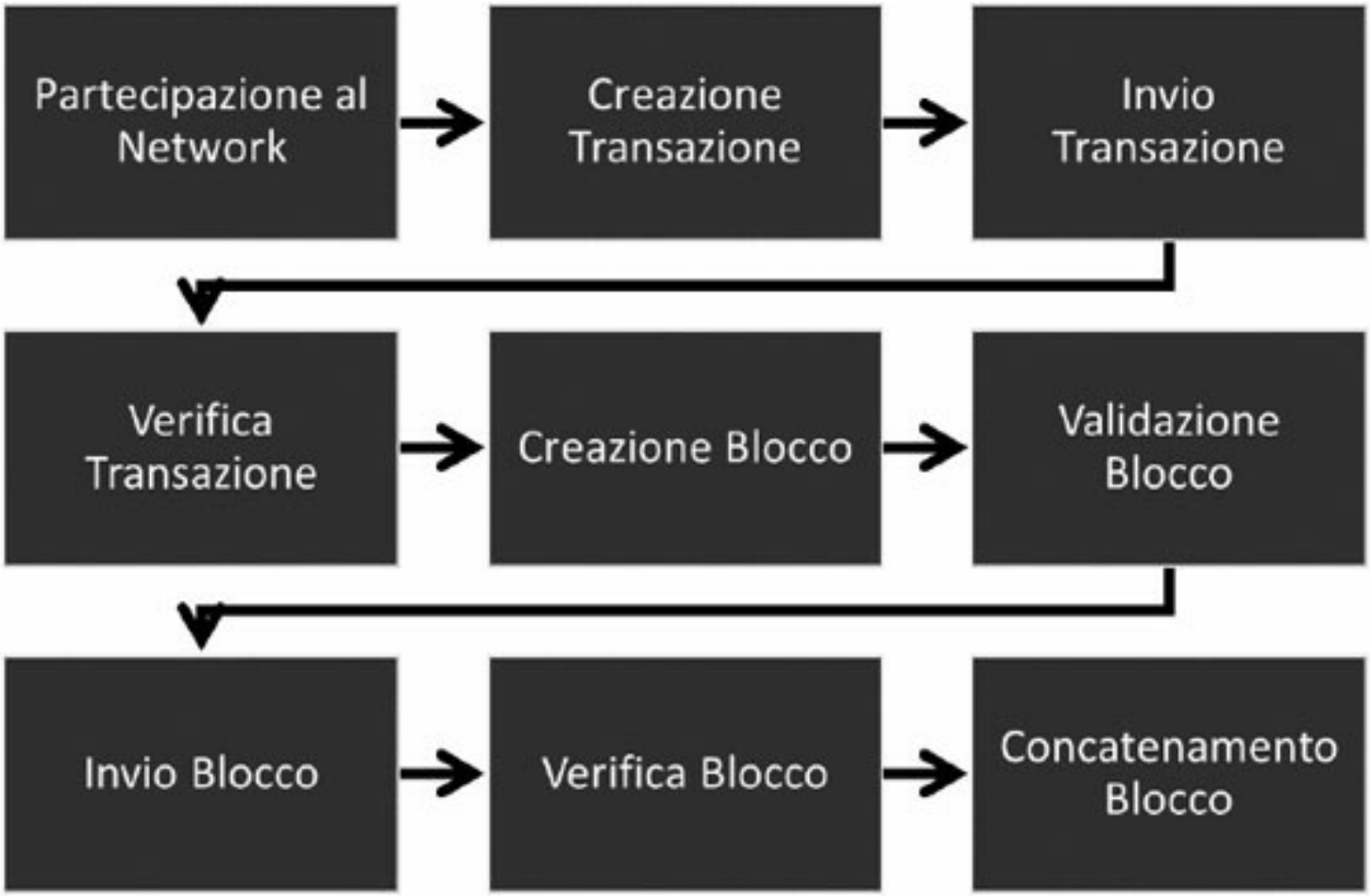

Figura 10.1 – Ciclo di vita di una transazione sulla Blockchain.

Come si sviluppa una transazione sulla Blockchain

Sulla Blockchain le transazioni servono a scambiare le proprietà di criptoasset tra i diversi partecipanti. Una transazione inizia con la sua creazione e, subito dopo, viene firmata digitalmente con una (o più) firme, al fine di dimostrare l'autorizzazione a spendere una certa parte di criptoasset (valorizzata nell'importo) riferita dalla transazione stessa. La transazione viene quindi inviata al network e verificata dai nodi che la

propagheranno a tutti gli altri. Infine, la transazione sarà validata da un nodo miner e inclusa in un blocco di transazioni registrato sulla Blockchain. Una volta registrata sulla Blockchain e confermata da un sufficiente numero di blocchi susseguenti, la transazione verrà permanentemente agganciata alla Blockchain e sarà accettata come valida da tutti i partecipanti. La disponibilità di criptoasset assegnata al nuovo proprietario dalla transazione potrà essere spesa – ovvero scambiata – in una nuova transazione, estendendo la catena di passaggi di proprietà e iniziando nuovamente il ciclo di vita di una transazione.

Partecipazione al

network

I partecipanti alla Blockchain sono un gruppo di computer (o, più in generale, di device interconnessi) che fanno parte di un network e ai quali ci si riferisce comunemente con il termine "nodo". Nella Blockchain di cui stiamo parlando qualsiasi nodo può liberamente collegarsi[44].

È importante sottolineare come la struttura della Blockchain in esame si differenzi da un sistema centralizzato (tipico della fase 1 di Welthyland, per capirsi). In un sistema centralizzato le transazioni vengono registrate da una terza parte che detiene e gestisce l'unico ledger autorizzato. Nella Blockchain

invece ogni nodo ha una copia del ledger sincronizzata localmente (Figura 10.2) e non vi è la necessità di una terza parte centralizzata.

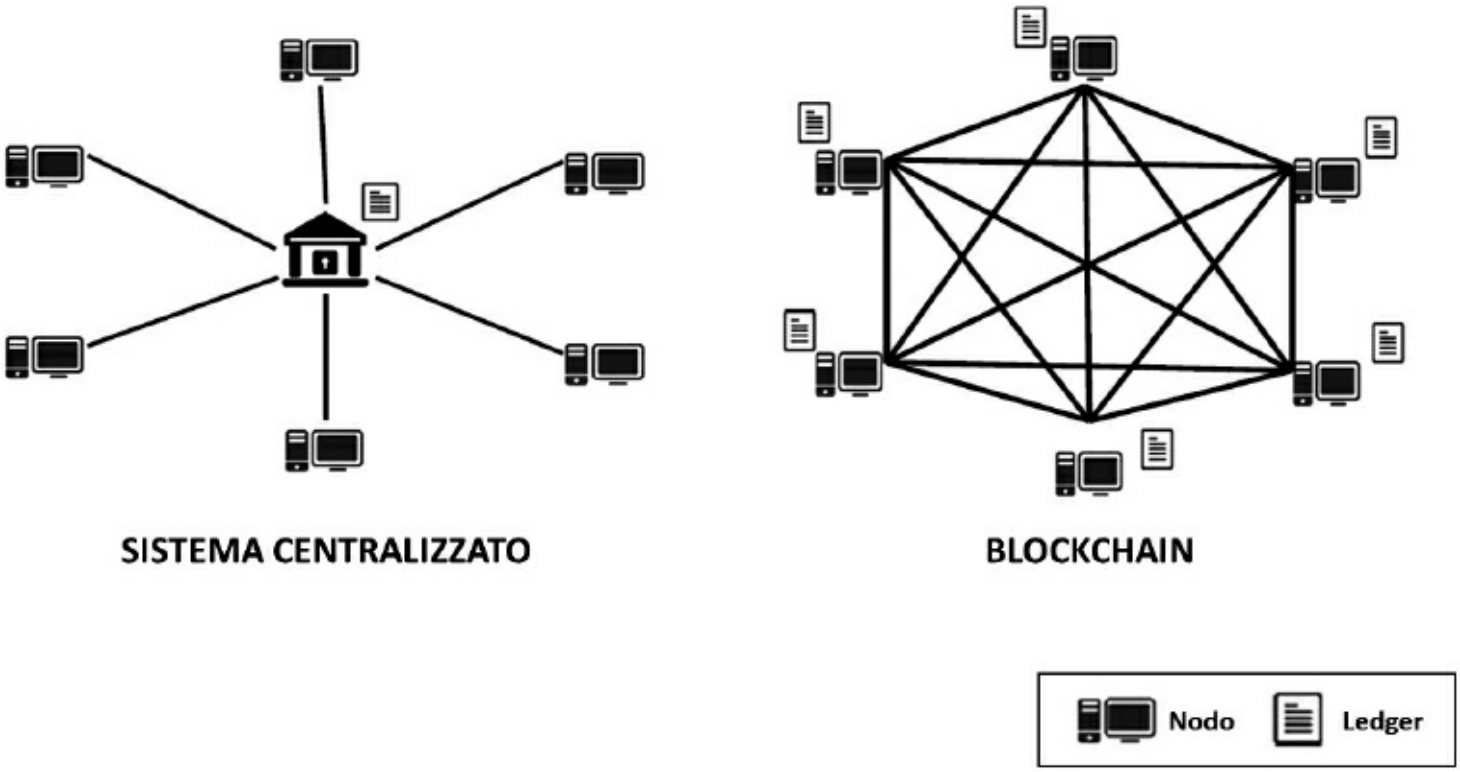

Figura 10.2 – Confronto fra sistema centralizzato e Blockchain.

La creazione di una transazione sulla Blockchain

Effettuare una transazione fra due parti sulla Blockchain significa scambiare "Unità di Valore" (o criptoasset). Un soggetto "cedente" che vuole trasferire "Unità di Valore" a un soggetto "cessionario" deve creare una transazione firmandola con la propria chiave privata. La Figura 10.3 mostra un esempio di transazione fra Alice, cedente il criptoasset (1 "Unità di Valore"), e Bob, cessionario.

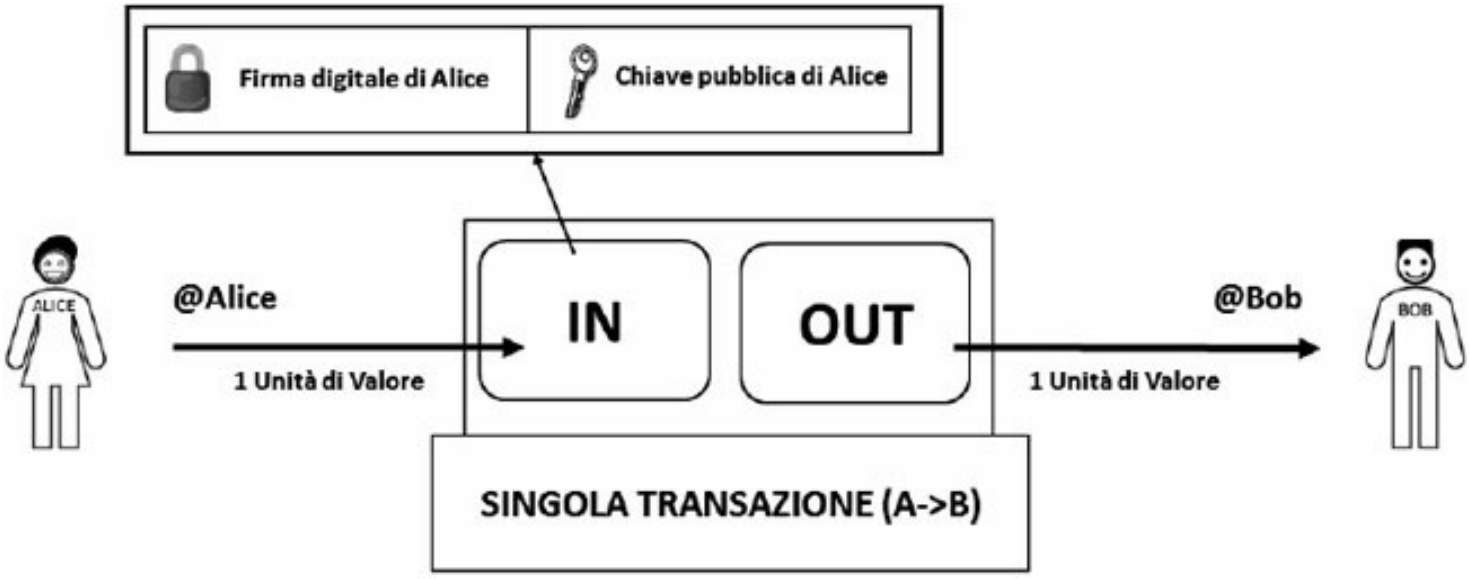

Figura 10.3 – Creazione di una transazione sulla Blockchain.

La funzione di Hash

La funzione di Hash è un sistema matematico che consente di convertire un messaggio di lunghezza arbitraria in un messaggio in codice alfanumerico di lunghezza fissa (o prefissata) chiamata Digest o impronta digitale. Tra le

funzioni di Hash più frequentemente impiegate figurano: MD4 (Message Digest 4), MD5 (Message Digest 5), SHA (Secure Hash Algoritm). L'impronta digitale è tale da identificare in modo univoco e irreversibile il messaggio iniziale garantendone integrità e autenticità. Nella Figura 10.4 viene riportato un esempio esaustivo di come la funzione di Hash sia in grado di garantire queste proprietà (l'algoritmo che ci interessa è lo SHA-256[45]). Se si cambia anche solo un carattere (nel nostro esempio la "a" semplice con la "à" accentata della stringa "1 Unità di Valore"), si ottiene un codice Hash completamente diverso.

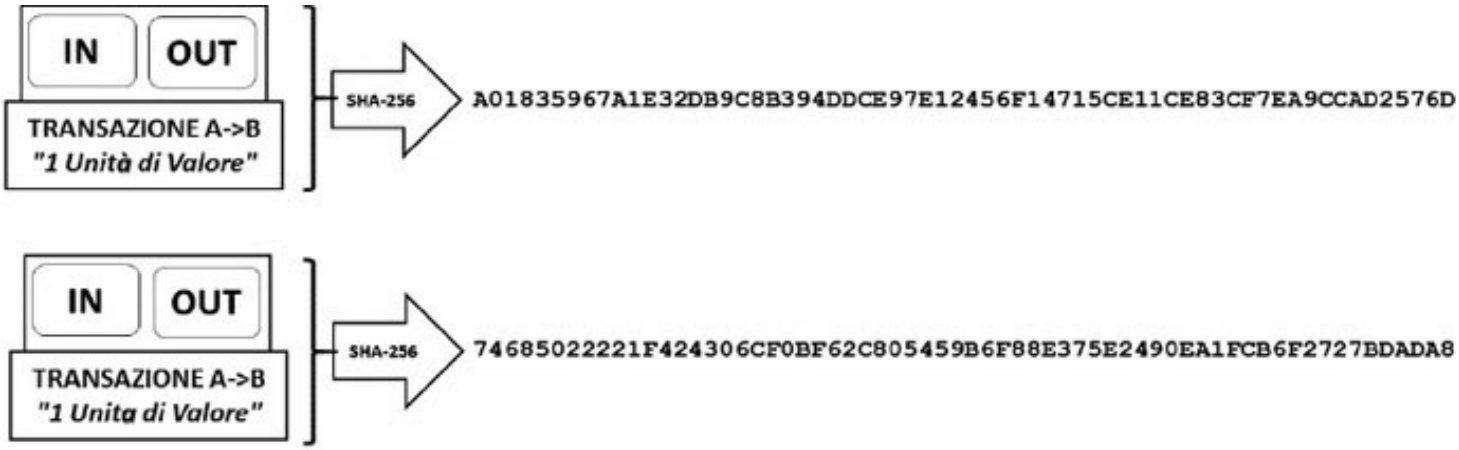

Figura 10.4 – Applicazione della funzione di Hash (SHA-256).

La creazione del Digest e la firma digitale

Quando un nodo crea una transazione (per esempio perché Alice, tramite il suo wallet, ha avviato lo scambio che abbiamo visto nella Figura 10.3), prima

di inviarla agli altri nodi esegue queste procedure:

- crea il Digest della transazione applicando la funzione di Hash;
- firma il Digest usando la chiave privata del mittente (ossia Alice, nel nostro caso), ottenendo così la firma digitale della transazione;
- aggiunge la chiave pubblica del destinatario (ossia Bob).

Quando Bob riceverà la transazione, essendo a conoscenza della chiave pubblica di Alice, sarà in grado di decifrare la firma digitale apposta dalla

medesima ottenendo il Digest; applicando la funzione di Hash alla transazione sarà quindi in grado di confrontare il risultato con il Digest creato da Alice e se i due valori combaciano significa che quella transazione è integra e autentica.

La chiave pubblica di Bob presente nella transazione servirà a Bob nel momento in cui vorrà spendere la disponibilità di criptoasset che gli è stata trasferita da Alice. Per fare questo Bob dovrà ripetere lo stesso procedimento descritto per Alice, ossia, supponendo che voglia eseguire una transazione a beneficio di Dan, dovrà creare il Digest applicando la funzione di Hash, firmarlo con la sua chiave

privata e aggiungere la chiave pubblica di Dan. Dan, a propria volta, potrà verificare che la transazione proviene da Bob, essendo a conoscenza della sua chiave pubblica e attuando così la medesima procedura di verifica dell'autenticità della transazione posta in essere da Bob quando aveva ricevuto da Alice la disponibilità di criptoasset conferitagli.

Qualora Bob non fosse quello che dice di essere, ossia pensasse di usare la disponibilità trasferita da Alice pur non essendo il beneficiario legittimo della transazione, non potrebbe usare la propria chiave privata per firmare la transazione a beneficio di Dan: questo

perché in realtà la disponibilità di criptoasset trasferita da Alice è "bloccata" sul vero Address di Bob (la chiave pubblica di Bob presente nella transazione originata da Alice) consentendo solo all'autentico Bob di poterla sbloccarla con la sua chiave privata. Questo procedimento vi sarà più chiaro quando spiegheremo cosa sono gli UTXO e gli script di transazione, nei paragrafi di questo capitolo "Cosa sono gli UTXO nella Blockchain" e "Gli Output e gli Input di una transazione".

La transazione Root (o

Root Transaction)

Nella Blockchain la Root Transaction (Tx_Root) si ottiene applicando successivamente e ricorsivamente la funzione di Hash a un insieme di transazioni secondo uno schema ad albero di Merkle (Merkle Tree). In questo modo si ha la certezza dell'integrità e autenticità di più transazioni raggruppate ad albero (Figura 10.5). Ritroveremo la transazione di Root più avanti, quando spiegheremo la creazione di un blocco.

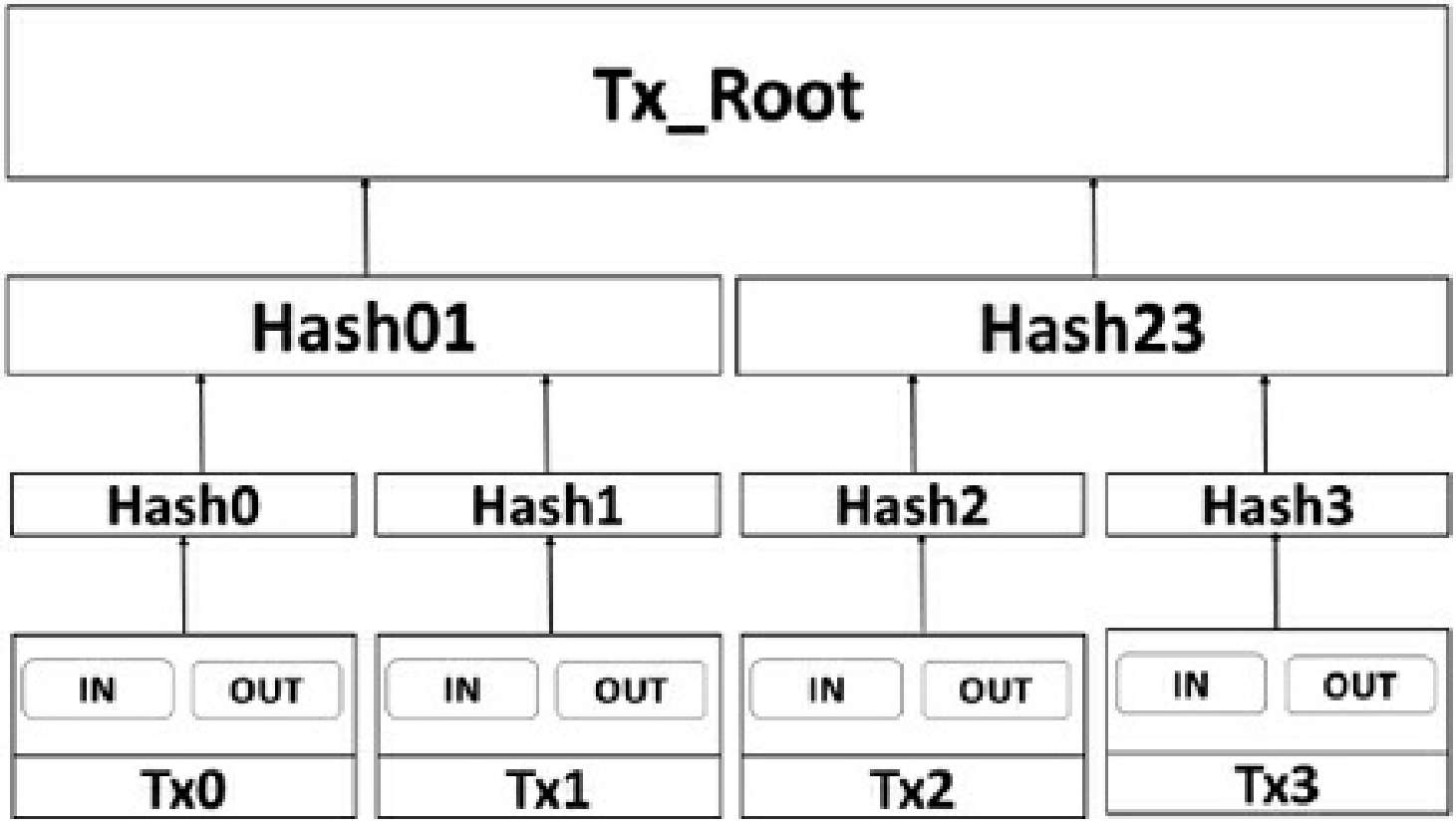

Figura 10.5 – Raggruppamento degli Hash di più transazioni nella Root Transaction (Merkle Tree).

La struttura di una transazione

Una transazione può essere rappresentata come una struttura dati che

codifica e trasferisce un valore (numericamente quantificato dall'importo di criptoasset presente nella transazione) da una sorgente chiamata "Input" a una destinazione chiamata "Output". Gli Input e gli Output non sono relazionati a nessun conto così come non sono legati ad alcuna identità, se non quella rappresentata dalle chiavi pubbliche dei partecipanti. Esattamente come abbiamo spiegato con la metafora di Welthyland, dove non esiste il concetto di "conto", possono essere intesi come "pezzi di bitcoin" (in Welthyland erano Welthy) tra di loro correlati e protetti mediante una chiave segreta (la chiave privata) che solo il

proprietario, o la persona che conosce la chiave, può sbloccare.

Cosa sono gli UTXO nella Blockchain

I componenti fondamentali di una transazione in criptoasset sulla Blockchain sono i cosiddetti “Unspent Transaction Outputs” (Output di transazione non spesi) o “UTXO”. Gli UTXO sono frammenti indivisibili di criptoasset “annodati” a uno specifico proprietario, registrati sulla Blockchain e riconosciuti come unità di valore da tutto il network. Sul Distributed Ledger

dei bitcoin sono tracciati tutti gli UTXO disponibili (ossia non spesi) e ogniqualvolta un partecipante riceve bitcoin, quella somma viene registrata sulla Blockchain come UTXO. Pertanto, la disponibilità di criptoasset di un partecipante è come se fosse sparpagliata in UTXO nelle migliaia di transazioni e migliaia di blocchi. Come raccontato con la metafora di Welthyland, nella Blockchain non esiste il concetto di "saldo" associato a un "conto" (non c'è neppure il concetto di "conto", come accennato poc'anzi) ma ci sono solo UTXO disseminati, dei quali gli specifici proprietari sono in grado di dimostrare la proprietà[46],

ovvero la disponibilità.

Gli Output e gli Input di una transazione

Ogni transazione sulla Blockchain crea Output registrati sul Distributed Ledger, ossia scrive UTXO che potranno essere usati dal cessionario, nel rispetto di alcune regole programmabili che vedremo meglio nel prossimo capitolo, dedicato al linguaggio di scripting della Blockchain. Trasferire la disponibilità di cripto-asset da Alice a Bob significa originare una transazione che registra UTXO associandoli all'Address di Bob.

Gli UTXO sono tracciati da ogni nodo come serie di dati chiamata “UTXO set” (o “UTXO pool”), salvata in un database. Le nuove transazioni “consumano” (spendono) uno o più di questi output dal set di UTXO. Gli UTXO “consumati” da una transazione su Blockchain sono chiamati Input della transazione, mentre gli UTXO “creati” da una transazione sono chiamati Output della transazione. In questo modo, porzioni di valore si trasferiscono da un proprietario all’altro in una catena di transazioni che consumano e creano UTXO.

Le transazioni consumano UTXO “sbloccandoli” con la firma del proprietario attuale e creano UTXO

“bloccandoli” sull’Address di un nuovo proprietario.

L’eccezione alla catena di Output e Input è un tipo speciale di transazione chiamata “coinbase”, che è la prima transazione in ogni blocco. Questa transazione è immessa sulla Blockchain dal miner “vincitore” (ossia colui che dimostra la Proof-of-Work validando il blocco) creando, di fatto, nuove unità di valore disponibili per quel miner come ricompensa per aver effettuato il lavoro di mining. Questo è l’unico modo con cui è possibile creare nuovi criptoasset, esattamente come spiegavamo nella fase 3 di Welthyland quando ci riferivamo al concetto di “deposito” sulla Blockchain.

La struttura di un Output di transazione

Gli Output di transazione sono rappresentati in una struttura dati che contiene (almeno):

- un importo utilizzato per valorizzare la quantità di criptoasset trasferita coincidente con gli UTXO;
- un campo chiamato “Locking-Script”[47] (o script di blocco), che blocca gli UTXO specificando le condizioni che devono essere soddisfatte per consentire al cessionario, ossia il destinatario della

transazione, di disporne liberamente;

- una marcatura temporale (o “timestamp”).

La struttura di un Input di transazione

Gli Input di transazione sono rappresentati in una struttura dati che contiene (almeno):

- un puntatore a UTXO referenziati con il Digest della transazione, calcolato applicando la funzione di Hash (in sostanza punta al precedente Output di una

transazione, che, ricordiamo, include anche il timestamp);

- un numero di sequenza in cui l'UTXO è registrato nella Blockchain (in sostanza è un ulteriore puntatore al precedente Output di una transazione);
- un campo chiamato "Unlocking-Script"[48] (o script di sblocco).

Per utilizzare UTXO, un Input di transazione include anche script di sblocco che soddisfano le condizioni di spesa impostate dall'UTXO. Lo script di sblocco è solitamente una firma digitale

che dimostra la proprietà dell'Address inserito nello script di blocco del precedente Output.

L'invio di una transazione ai nodi del network

Quando un nodo ha creato una transazione (per esempio perché Alice, tramite il suo wallet, ha avviato lo scambio che abbiamo visto nella Figura 10.3), ne calcola il Digest applicando la funzione di Hash che abbiamo spiegato in precedenza e illustrato nella Figura 10.4. L'Hash (nel cui calcolo è incluso

anche il timestamp della transazione) e la transazione vengono propagati agli altri nodi del network (Figura 10.6) per consentire l'avvio del processo di verifica. Tale processo (che spiegheremo nel successivo paragrafo) è anche chiamato "processo di verifica indipendente" poiché questa fase, precedente a quella di validazione che si avrà con il mining del blocco, è operata da ciascun singolo nodo senza – ancora – doversi preoccupare di cosa stiano facendo nello stesso istante (e magari sulle medesime transazioni) gli altri, ossia senza incaricarsi di raggiungere quel consenso distribuito che abbiamo descritto nella fase 3 di Welthyland, operazione che avverrà successivamente

alla presentazione della Proof-of-Work del miner vincitore (ovvero il risolutore del puzzle crittografico).

La verifica di una transazione sulla Blockchain

Ogni transazione viene rappresentata dalla propria storia, esattamente come avevamo descritto per Welthyland (in tutte e tre le sue fasi) nel Capitolo 5 al paragrafo “Un modo alternativo per controllare la reale disponibilità di Welthy non spesi”. Con questo sistema qualsiasi nodo che accede al network è

in grado di verificare se il cedente che ha avviato la transazione (Alice, nel nostro esempio) ha realmente la disponibilità dei criptoasset che sta trasferendo al cessionario (Bob). La Figura 10.7 illustra come avviene la verifica delle transazioni andando a ritroso a partire dall'ultima transazione.

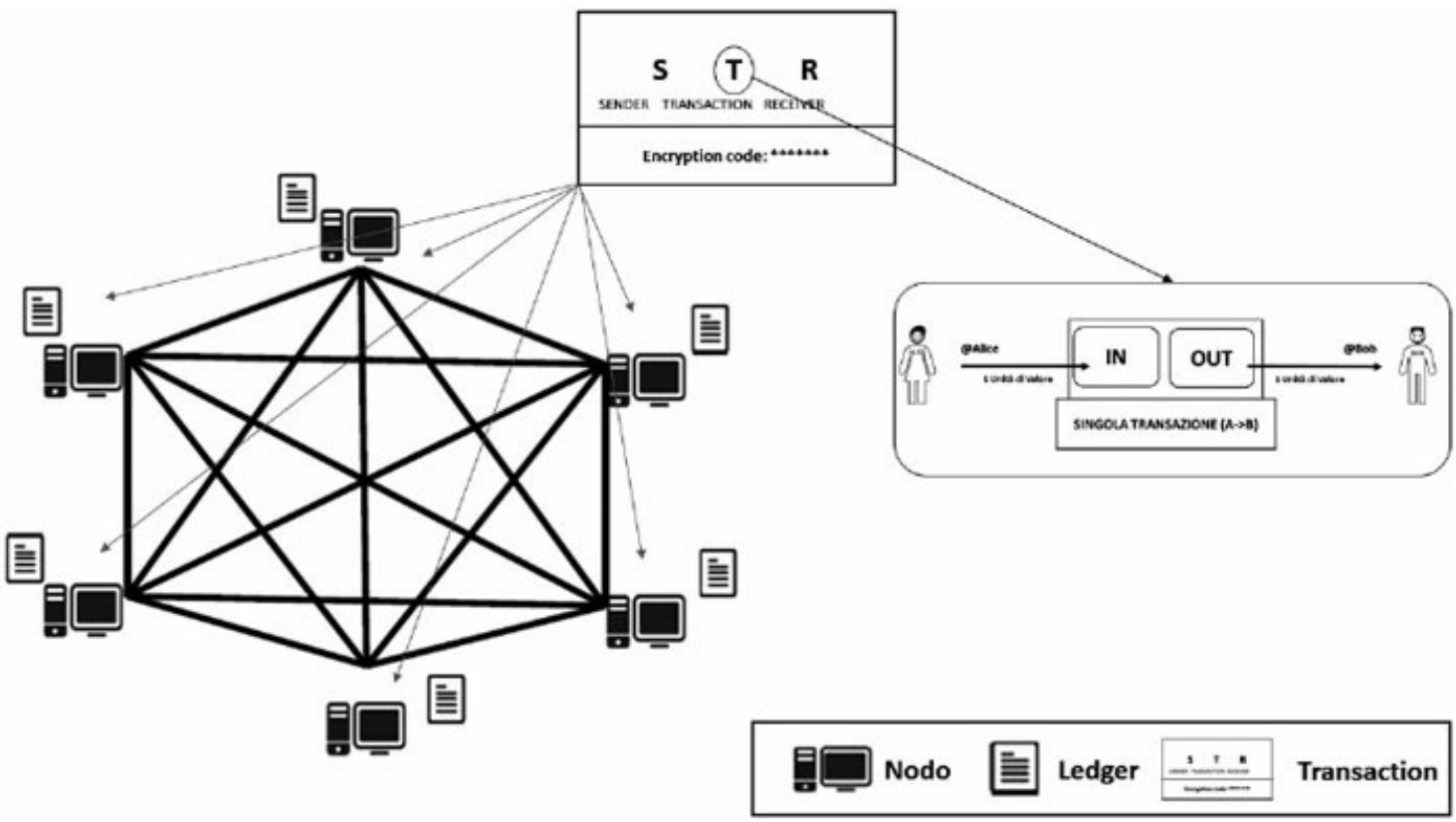

Figura 10.6 – La propagazione di una transazione nel network.

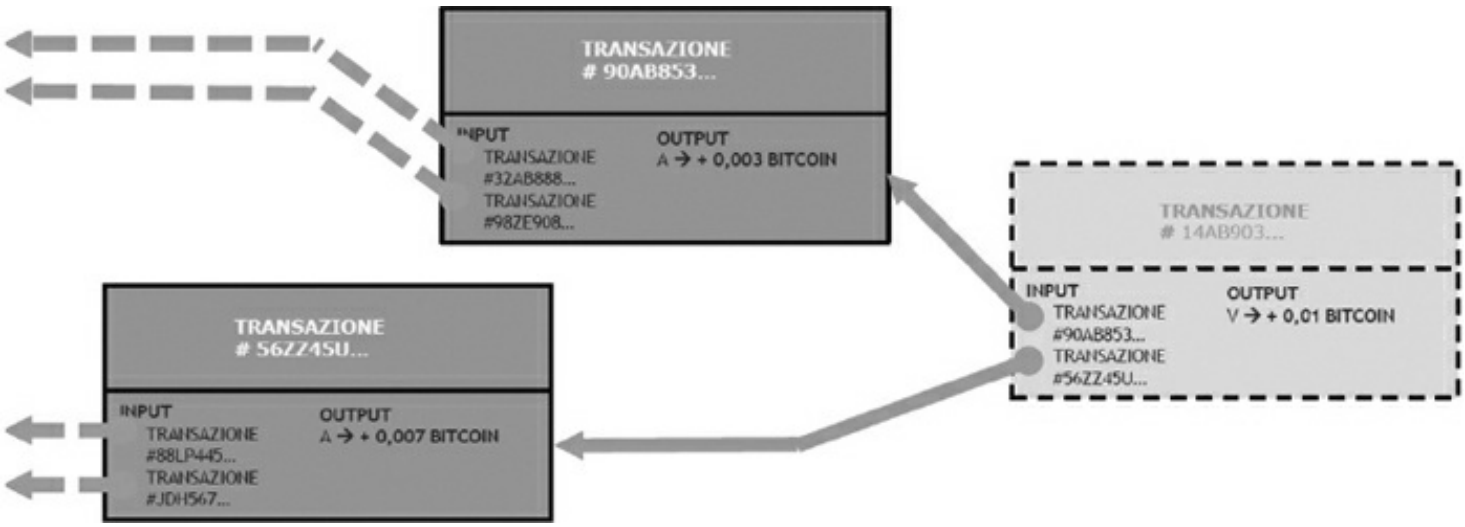

Figura 10.7 – La verifica di una transazione.

La creazione di un blocco sulla Blockchain

Quando un nodo riceve una transazione

verificata, inizia a "costruire" un blocco che al suo interno includerà tutte le successive transazioni che, con il tempo, si andranno propagando sulla Blockchain (Figura 10.8).

Entrando nel dettaglio di un singolo blocco, troveremo diverse transazioni verificate che sono in attesa di conferma, ossia sono all'interno di un blocco che non è ancora stato validato. Poiché abbiamo detto che quando un blocco viene validato mediante il processo di mining (che spiegheremo nel successivo paragrafo) è aggiunto dagli altri nodi alla catena, nella Figura 10.9 mostriamo l'anteprima di una catena, che ha il solo scopo di farvi vedere come, in un determinato istante, in un

nuovo blocco possano trovarsi transazioni verificate ma non ancora validate (in attesa di conferma). In particolare, avremo che nel blocco #504968, non ancora validato, vi sono delle transazioni in attesa, mentre nei precedenti blocchi #504967 e #504966, già validati, si trovano delle transazioni confermate.

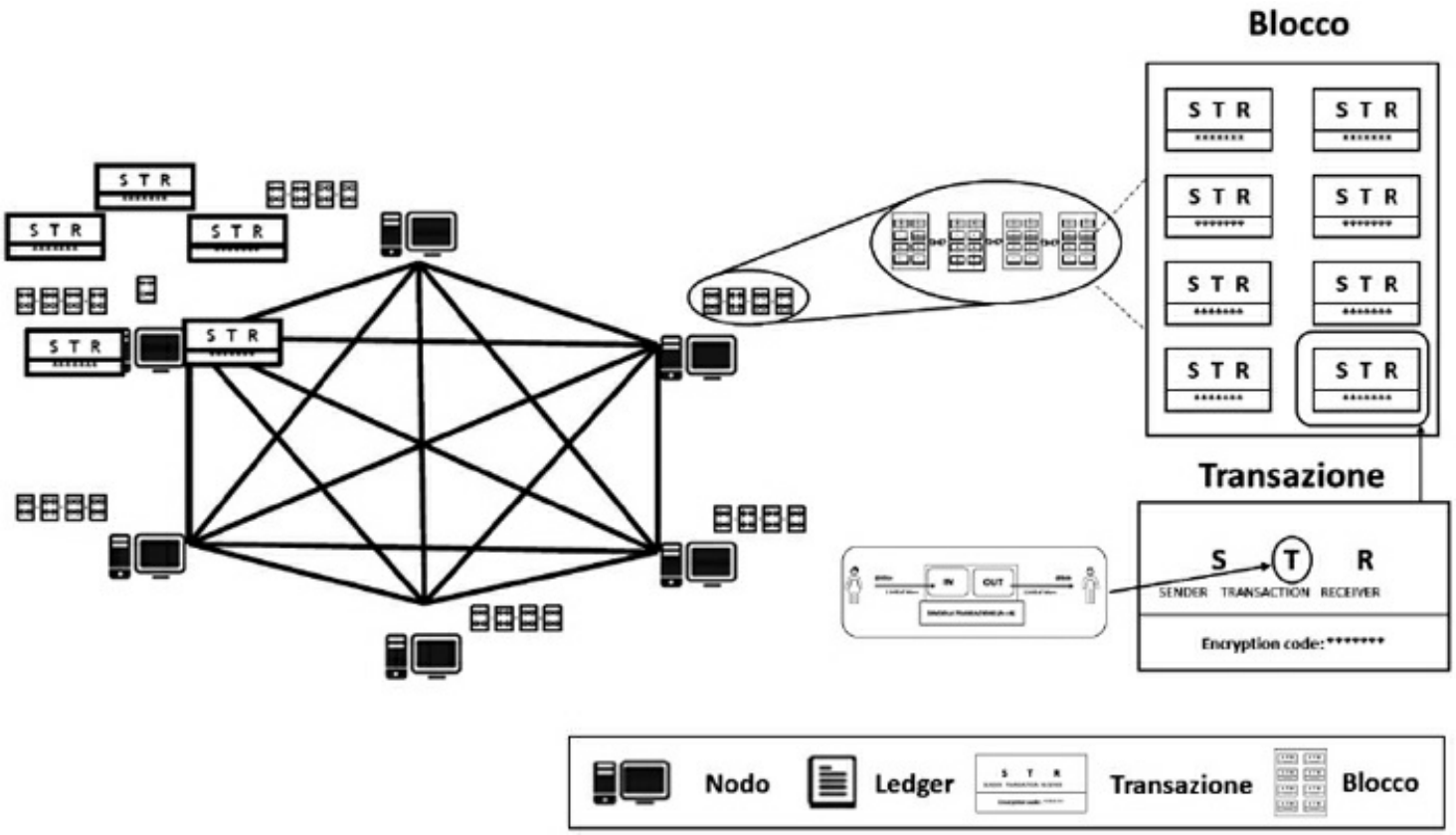

Figura 10.8 – La costruzione di un blocco.

Sempre nella Figura 10.9 abbiamo aggiunto i risultati della funzione di Hash applicata ai due nodi validati e la transazione di Root ottenuta sulle transazioni contenute nel singolo blocco, applicando successivamente e ricorsivamente la funzione di Hash

all'insieme delle transazioni secondo uno schema ad albero di Merkle (Merkle Tree), come descritto nel precedente paragrafo di questo capitolo "La transazione Root (o Root Transaction)"[49]:

- Hash del blocco #504967 –> 00000000000000000732efc6…
- Hash del blocco #504966 –> 00000000000000006b75bbf98…
- Transazione di Root (Merkle Tree) delle transazioni validate contenute nel blocco #504967 –> 03f76fca28241f…
- Transazione di Root (Merkle Tree) delle transazioni validate

contenute nel blocco #504966 –> 29d2dad0c3b237…

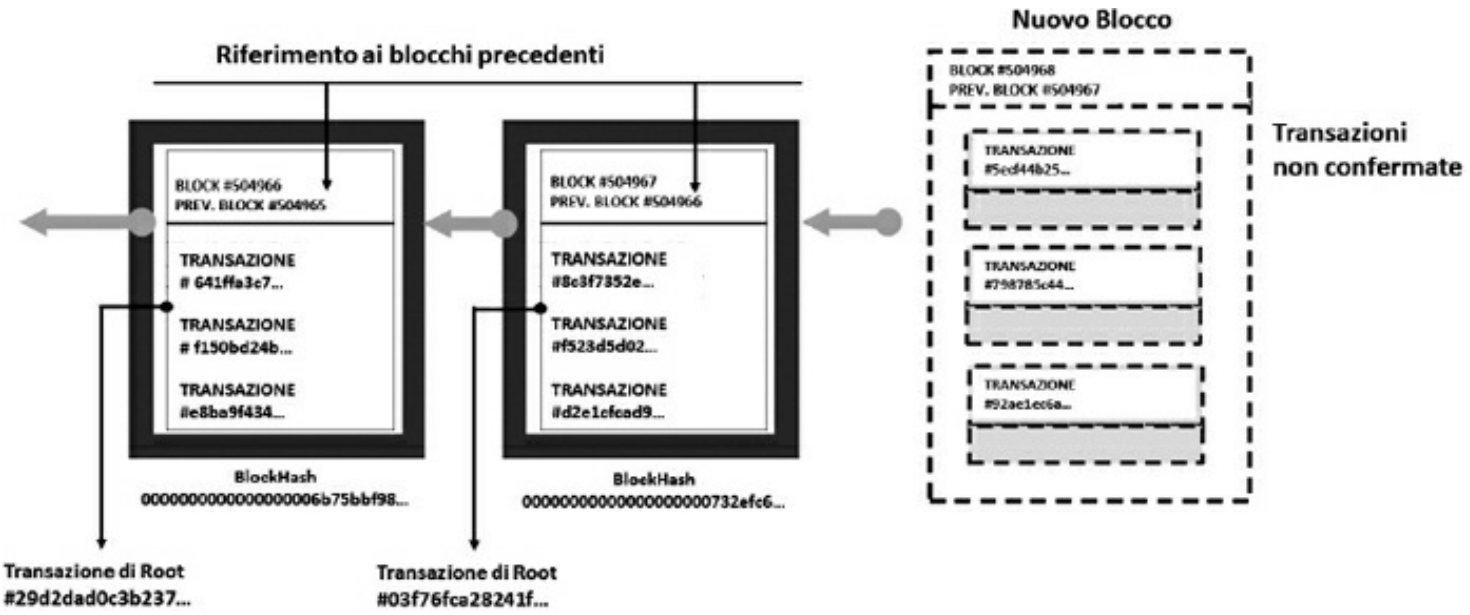

Figura 10.9 – La generazione di un nuovo blocco.

La validazione di un blocco sulla Blockchain

Quando un nodo riceve una transazione verificata e si accinge a "costruire" un blocco come abbiamo visto nella Figura 10.8, inizia quel processo di validazione (altresì chiamato "mining") che consta nel partecipare alla competizione con gli altri nodi, al fine di risolvere per primo un puzzle crittografico, similmente a quanto avevamo descritto nella fase 3 di Welthyland al paragrafo "La prova di lavoro per la validazione delle pagine di un registro distribuito" (Capitolo 6).

Tale attività è potenzialmente avviabile da qualsiasi nodo validatore che, mentre riceve le transazioni verificate che si stanno propagando lungo il network (come abbiamo

spiegato nel precedente paragrafo), decide di candidarsi per gareggiare con altri nodi validatori nella presentazione della Proof-of-Work.

Ogni blocco presenta un Header (o testata) che lo identifica sulla base della valorizzazione (almeno) dei seguenti campi:

- **Numero del blocco** (o "**Height**"): indica la posizione – o altezza – del blocco nella catena.
- **Timestamp**: è una marcatura temporale che segna la creazione del blocco.
- **Merkle Root**: è un campo che

viene valorizzato con la Root Transaction, che abbiamo descritto nel precedente paragrafo di questo capitolo "La transazione Root (o Root Transaction)" e illustrato nella Figura 10.5.

- **Nonce**: è una stringa casuale di dati che viene utilizzata nel processo di hashing di un blocco; viene utilizzato un nonce diverso per ogni tentativo di hashing, al fine di soddisfare il target richiesto nel processo di mining di un blocco.
- **Target difficulty**: è un numero

estremamente grande (a 256 bit), il cui valore si modifica in base al tempo effettivo e teorico necessario per validare 2.016 blocchi (più il target è piccolo e più è difficile ricercare una soluzione che lo possa soddisfare); correlato alla difficoltà, rappresenta la misura di quanto sia complicato trovare un Hash al di sotto di un certo target. Nella Blockchain dei Bitcoin non può essere inferiore a 1 e viene aggiustato ogni 2.016 blocchi, ossia mediamente ogni 12 giorni.

- **Previous Hash**: rappresenta l'Hash del blocco precedentemente validato e verificato, ossia il blocco che precede nella catena di una sola posizione rispetto al blocco in esame.
- **Version**: indica la versione del protocollo attualmente impiegato per minare i blocchi sulla catena[50].

Si notino alcune rassomiglianze dei campi presenti nell'Header di un blocco con quelli che identificano le singole transazioni spiegati nel precedente paragrafo di questo capitolo "La struttura di una transazione". In

particolare, si osservi come nell'Header di un blocco non esista un riferimento al successivo blocco. La catena è, infatti, costruita basandosi sul solo riferimento al blocco precedente, ciò perché nel momento in cui un nodo validatore risolve il puzzle crittografico non sa ancora se gli altri nodi potranno avvalorarne la corretta soluzione, aggiungendolo così alla catena (processi descritti nei successivi paragrafi). Solo quando gli altri nodi verso i quali propagherà la Proof-of-Work – veicolando il valore del nonce che soddisfa il target – verificheranno la sua effettiva correttezza, potrà ritenere valida la sua ricompensa (che lo remunera per il lavoro di validazione

effettuato).

Nella Figura 10.10 viene riportata una semplice raffigurazione della catena di blocchi, riprendendo i medesimi che comparivano nella Figura 10.9[51].

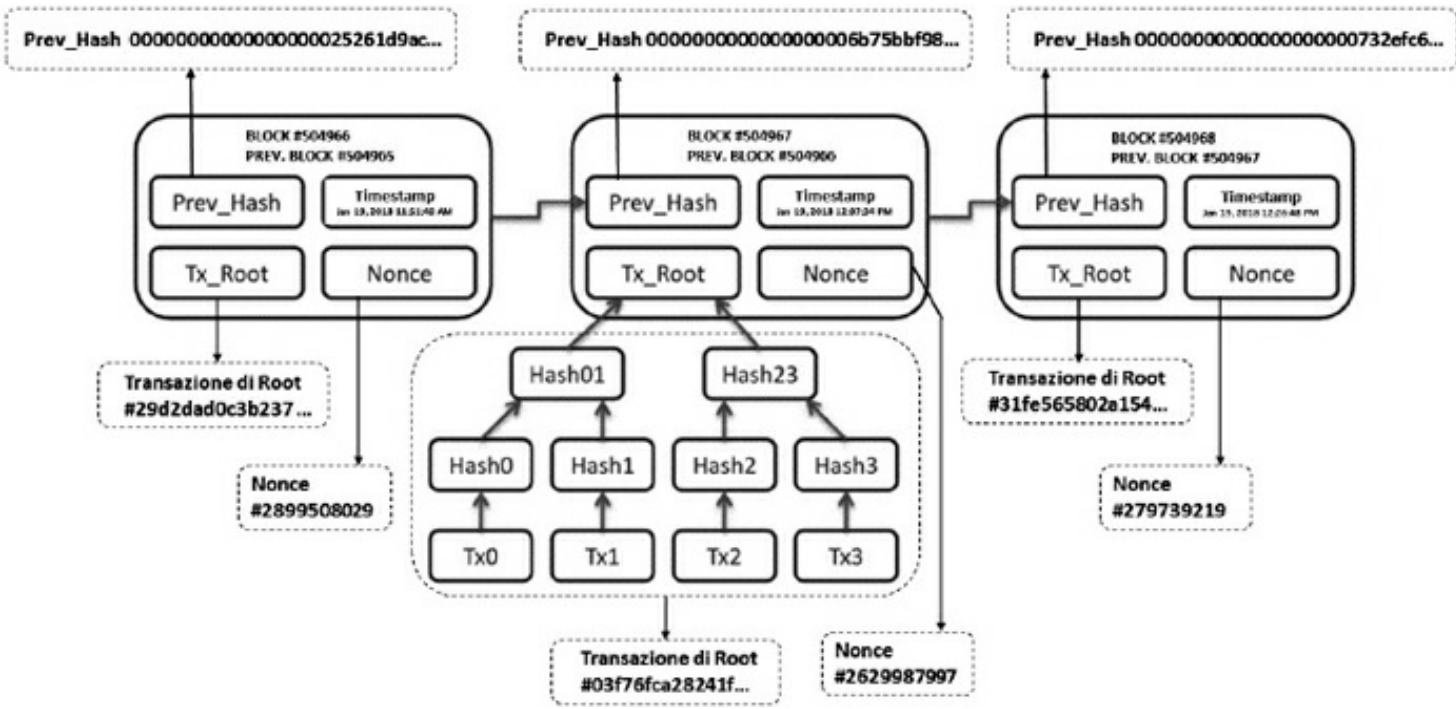

Figura 10.10 – Rappresentazione di una catena di blocchi validati.

L’attività di mining

Per validare i blocchi, la Proof-of-Work che i nodi devono presentare al fine di ottenere la ricompensa (e le mance) consta nel risolvere un puzzle crittografico molto complicato, lungo e costoso in termini di energia elettrica che deve essere continuamente erogata per supportare i server e la loro potenza computazionale. Per tali caratteristiche il processo viene anche chiamato “mining”, con riferimento all’attività svolta dai minatori per estrarre l’oro. In realtà non si tratta di alcuna “estrazione”, bensì di un gioco matematico che pone in competizione i

nodi validatori (o “miner”) e che ricompensa il vincitore tramite la validazione della transazione di reward, con le modalità descritte nei precedenti paragrafi “Gli incentivi per i validatori delle transazioni su un registro distribuito” (nella metafora di Welthyland in fase 3, Capitolo 6) e “Gli Output e gli Input di una transazione” (nel caso dei Bitcoin, in questo stesso capitolo).

La Proof-of-Work dei Bitcoin (ossia la validazione dei blocchi sulla Blockchain) consiste nel creare un Hash che, obbligatoriamente, presenti una specifica serie di valori, per esempio che inizi con la stringa “0000000”. Ogni nodo deve trovare quel valore che,

aggiunto alle altre transazioni, permetta di ottenere il risultato richiesto. Tale valore si chiama “nonce” (number once) e, continuamente modificato, porterà alla creazione di un Hash come richiesto[52].

Nella Figura 10.11 abbiamo illustrato il processo di validazione del blocco, in continuità con quanto rappresentato nelle precedenti Figure 10.6 e 10.8.

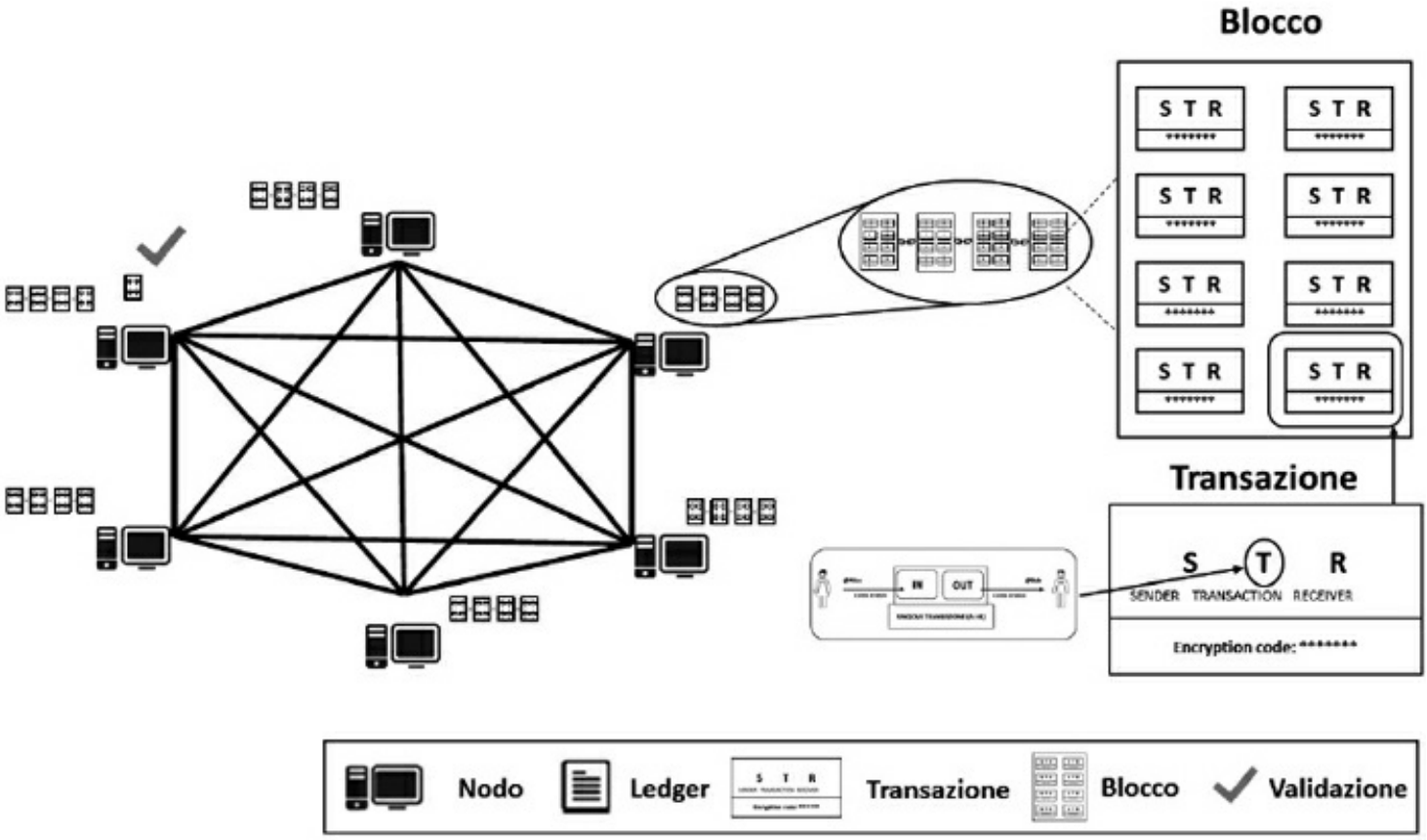

Figura 10.11 – La validazione di un blocco.

Come evitare il "Double Spending" sulla Blockchain

Poiché ogni nodo contiene le stesse

informazioni degli altri e, in questo modo, conosce la storia delle transazioni avvenute (al pari di tutti gli altri nodi), come si può essere certi che non siano validati blocchi che contengono transazioni mendaci? Se ci fosse un nodo che, surrettiziamente, provasse (riuscendovi) ad alterare la storia delle transazioni, inserendo una transazione falsa tale da ingenerare un problema circa la proprietà (o lo scambio di proprietà) dell'asset scambiato, si correrebbe il rischio del c.d. "Double Spending". Potrebbe succedere che il criptoasset trasferito da Alice a Bob, di cui Bob crede di avere la proprietà, fosse, un istante dopo il trasferimento da Alice, ri-attribuito ad

Alice, grazie all'intervento di un nodo che, volontariamente, alteri (in questo caso a discapito di Bob) la storia delle transazioni. Solo nel momento in cui Bob tentasse, a propria volta, di trasferire ad altri il criptoasset che crede suo, si accorgerebbe che è come se non ne fosse mai entrato in possesso (quindi potrebbe accorgersene anche dopo molto tempo). Per evitare l'azione fraudolenta di un nodo in malafede è necessario complicare il processo di validazione. Ogni nodo intenzionato a validare deve dimostrare di avere risolto un puzzle crittografico mettendosi in competizione con tutti gli altri nodi, per la soluzione del quale ognuno mette

a disposizione la propria potenza e capacità di calcolo. Solo il primo nodo che risolve il puzzle avrà diritto di validare il blocco, presentando la c.d. "Proof-of-Work" (ossia la soluzione del puzzle) e ricevendo in cambio una ricompensa in criptoasset. Su una rete Peer-to-Peer di nodi che non si conoscono fra di loro, questa attività che consente di pervenire a un consenso distribuito viene chiamata "mining" e rappresenta un possibile modo per raggiungere quella fiducia che, in assenza di un'autorità centrale, deve essere comunque conseguita, al fine di poter considerare valida la storia delle transazioni sulla Blockchain.

La propagazione dei blocchi sulla Blockchain

Una volta che il nodo validatore ha risolto la Proof-of-Work con le modalità che abbiamo descritto nei precedenti paragrafi e vincendo contro gli altri nodi, segnala al network il proprio blocco validato acciocché gli altri nodi possano verificarne l'effettiva correttezza.

La verifica dei blocchi sulla Blockchain

Una volta che la Proof-of-Work presentata dal nodo vincitore viene ricevuta dagli altri nodi, questi possono rapidamente appurarne l'esattezza, in un modo simile a quello spiegato nella fase 3 di Welthyland al paragrafo "La prova di lavoro per la validazione delle pagine di un registro distribuito" (Capitolo 6).

Nella Figura 10.12 abbiamo illustrato il processo di verifica di un blocco validato, in continuità con quanto rappresentato nelle precedenti Figure 10.6, 10.8, 10.11.

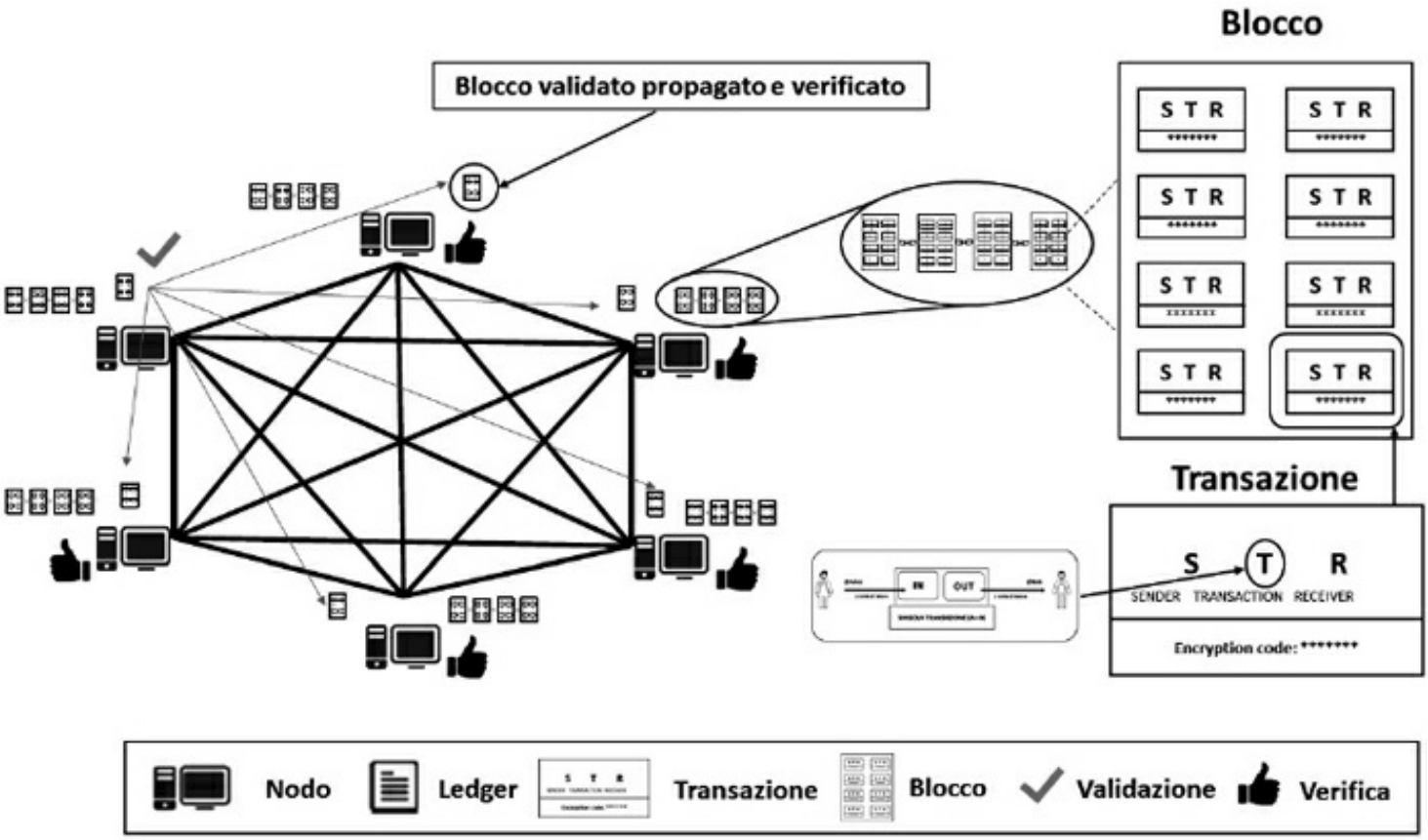

Figura 10.12 – La propagazione di un nodo validato e la verifica.

Il consenso distribuito su una blockchain pubblica

La fiducia (il “Trust”) su una blockchain come quella dei Bitcoin, ossia una blockchain dove l’accesso al Distributed Ledger è aperto a chiunque e senza la necessità di avere permessi stabiliti in una fase di predeterminazione e preassegnazione, viene creata rendendo particolarmente costosi i tentativi di manomettere la validazione del ledger, ovvero raggiungendo un consenso distribuito fra diversi miner mediante l’applicazione di regole comuni scritte nel protocollo. Se un miner disonesto (ossia in malafede) volesse validare una transazione falsa, dovrebbe competere con gli altri miner che agiscono onestamente, provando a

imporre un ordine diverso alle transazioni, ma dovendo ricalcolare tutte le Proof-of-Work prodotte fino a quel momento… e, ovviamente, tutto ciò dovrebbe cercare di farlo mentre altre transazioni vanno via via inserendosi in altri blocchi pronte per essere validate. Uno scenario possibile, ancorché teoricamente, è quello descritto con l'attacco del 51% che avevamo spiegato nel Capitolo 6, al paragrafo "Cosa potrebbe accadere nel caso di 'Double Spending'", e illustrato nella Figura 6.1.

Concatenazione dei blocchi sulla

Blockchain

Dopo che gli altri nodi hanno verificato il nodo validato, propagatosi nel network a seguito della presentazione della Proof-of-Work da parte del nodo validatore che ha risolto per primo il puzzle crittografico, esprimono il loro consenso (e l'accettazione del nuovo blocco) aggiungendolo alla catena e iniziando a creare il blocco successivo, impiegando l'Hash del blocco testé accettato quale riferimento al blocco precedente, esattamente come avevamo anticipato, illustrando graficamente, nella Figura 10.10.

Da questo momento in avanti riprende il processo sin qui descritto

con nuove transazioni verificate che saranno inserite in un nuovo blocco pronto per essere validato da un nuovo miner.

Nella Figura 10.13 abbiamo illustrato il processo di concatenazione di un blocco validato, propagato e verificato, in continuità con quanto rappresentato nelle precedenti Figure 10.6, 10.8, 10.11.

La risoluzione dei conflitti

Nel caso in cui due (o più) miner risolvessero nello stesso istante il

puzzle crittografico, ritenendo di aver così validato due (o più) blocchi che potrebbero anche contenere differenti transazioni verificate, gli altri nodi verso cui si propagherebbero le loro Proof-of-Work inizierebbero a lavorare sul primo blocco ricevuto, verificando l'esattezza della PoW e concatenandolo. Alla fine, la catena più lunga sarà quella che si impone e, come tale, verrà mantenuta (Figura 10.14).

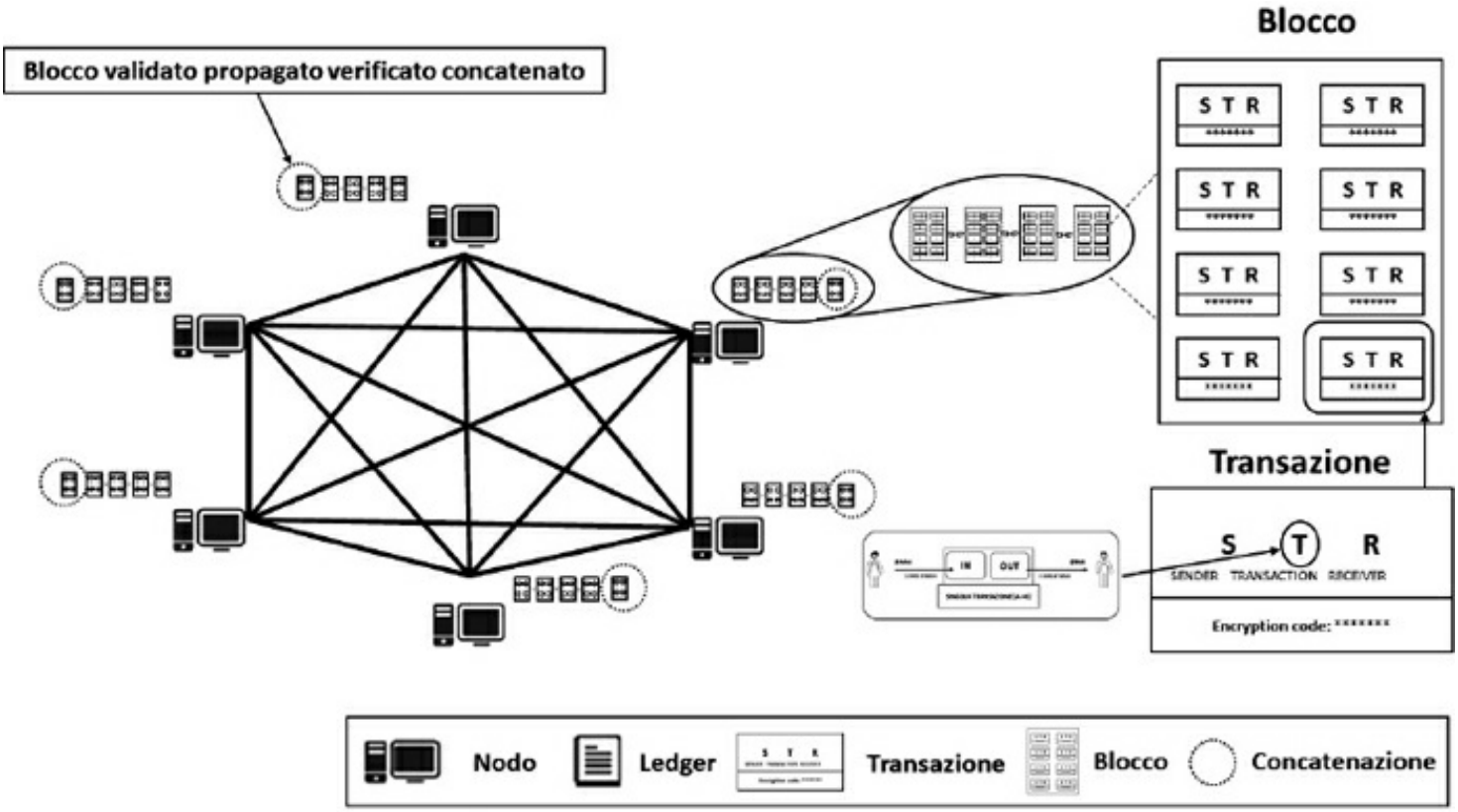

Figura 10.13 – La concatenazione di un blocco.

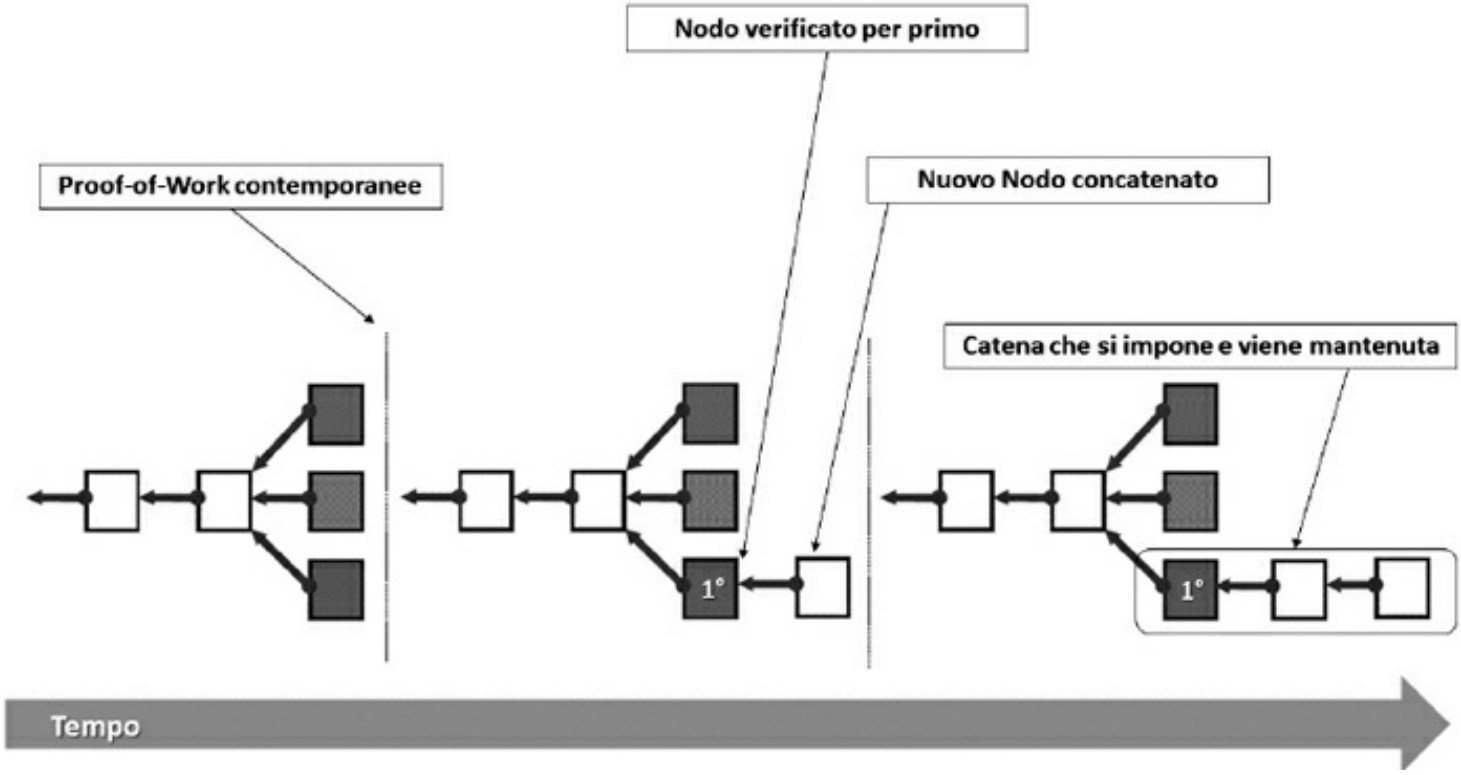

Figura 10.14 – La gestione dei conflitti.

---

44. Ricordiamoci sempre che stiamo parlando della Blockchain (con l'iniziale maiuscola) dei Bitcoin; in altre blockchain (come vedremo successivamente) l'accesso al network può essere condizionato.

45. L'algoritmo SHA è stato sviluppato dalla NASA (National Security Agency) e le specifiche sono state pubblicate dal NIST

(National Institute of Standards and Technology) nel 1993 (questa prima versione è nota come SHA-0). Nel 2001 sono state pubblicate quattro funzioni: SHA-224, SHA-256, SHA-384 e SHA-512. Queste funzioni sono frequentemente indicate come SHA-2.

46. Il concetto di "saldo bitcoin" di un partecipante è un costrutto derivato che viene creato dall'applicazione wallet del partecipante medesimo; il wallet calcola il saldo scansionando la Blockchain e aggregando tutti gli UTXO appartenenti a quel partecipante.

47. In molte applicazioni Bitcoin si chiama anche "ScriptPubKey".

48. In molte applicazioni Bitcoin si chiama anche "criptSig".

49. Nella Figura 10.9 per ragioni di stampa abbiamo riportato solo una parte dei valori risultanti dall'applicazione delle funzioni di Hash, che producono stringhe di caratteri

alfanumerici molto lunghe.

50. La versione del protocollo può cambiare a seguito di un accordo che è stato raggiunto dalla comunità di miner (si veda a tal proposito anche il successivo Capitolo 12, al paragrafo "Le Fork sulla Blockchain" e al box "I vulnus della e-democracy").

51. A chi volesse avere un dettaglio maggiore rispetto a quello riportato nella Figura 10.10, consigliamo di utilizzare un browser per navigare all'interno della blockchain dei Bitcoin (per esempio https://blockexplorer.com o https://www.smartbit.com.au) indicando i numeri dei blocchi che abbiamo riportato in figura.

52. Solo il miner più veloce nel risolvere il puzzle viene remunerato, gli altri devono continuare a competere per i blocchi successivi.

11

Il linguaggio di scripting della Blockchain

Come abbiamo visto nella Figura 10.3 e spiegato nel paragrafo “Gli Output e gli Input di una transazione”, contenuto nel precedente capitolo, una transazione sulla Blockchain prevede un Input e un

Output, i quali ci informano rispettivamente della provenienza (da Alice nel caso esaminato) e della destinazione (verso Bob nel caso in parola) del criptoasset scambiato.

Che cos'è uno script della Blockchain

Lo script è un microcodice scritto in uno specifico linguaggio di programmazione che accompagna le transazioni in modo da istruire i nodi

su che cosa fare dei dati ricevuti con le transazioni per realizzare operazioni più complesse del semplice trasferimento di criptoasset. L'esecuzione di uno script avviene anch'essa in modo distribuito, ossia ciascun nodo è in grado di eseguire lo script e di produrre un risultato tracciabile, non ripudiabile ed eternamente fissato (ossia scritto) sulla Blockchain.

All'interno degli Output e degli Input di transazione sono veicolati due script, rispettivamente chiamati "Locking-Script" e "Unlocking-Script", volti a determinare quali azioni devono essere compiute dai nodi che processano le transazioni in fase di verifica delle

stesse. Lo script non è altro se non un codice informatico (un piccolo programma, se preferite) che accompagna ogni transazione sulla Blockchain e per il quale ciascun nodo è in grado di eseguire specifiche azioni, finalizzate (per esempio) a consentire (o impedire) di usare la disponibilità di criptoasset trasferita da Alice a Bob.

Le caratteristiche funzionali di questo microcodice eseguito da ogni nodo sulla Blockchain permettono di conferire l'aggettivo "programmabile" al flusso di criptoasset (o, se preferite, criptovaluta) scambiati tra i diversi soggetti cedenti e cessionari. In pratica, con un'opportuna programmazione degli script mediante un linguaggio di

scripting apposito, è possibile determinare delle regole "agganciate" indissolubilmente all'asset nativo, che ne condizioneranno l'effettivo utilizzo. Nei successivi paragrafi proporremo alcuni esempi molto semplici che vi faranno comprendere come sia possibile condizionare gli scambi su una Blockchain. Per maggiore comprensione, laddove necessario, useremo il termine "bitcoin", riferendoci direttamente all'asset nativo della Blockchain. Cionondimeno, è importante chiarire che la programmabilità ottenuta tramite l'uso degli script può estendersi ad appannaggio di una specifica gestione dell'asset fisico, rendendo così

condizionabile, in funzione di regole predeterminate, il negozio giuridico sottostante alla transazione in criptoasset.

Uno script che regola la distribuzione di criptoasset ai soli bisognosi

Supponiamo che Alice stabilisca di trasferire la disponibilità di parte dei propri criptoasset (ossia i bitcoin) verso Bob, solo se Bob dimostra di esserne realmente bisognoso. Con uno script

speciale agganciato alla transazione, Alice può impedire a Bob di usare la quantità di criptoasset trasferita nel caso in cui l'UTXO set di questi (si veda il paragrafo "Cosa sono gli UTXO nella Blockchain", Capitolo 10) conti un valore superiore a una determinata cifra, ossia il livello d'indigenza per il quale Alice consente l'uso effettivo a Bob dei bitcoin trasferiti. Laddove tale livello non fosse soddisfatto, Bob potrebbe essere in grado di ricevere i bitcoin correttamente (in definitiva Bob è il beneficiario – o cessionario – di cui Alice conosce le generalità, ovvero la chiave pubblica associata al suo Address) ma non potrebbe a propria volta disporne liberamente, ossia non

potrebbe “spenderli” scambiandoli con altri.

Uno script che regola l’uso di criptoasset in specifici contesti

Supponiamo che Alice decida di trasferire la disponibilità di parte dei propri criptoasset (ossia i bitcoin) verso Bob, solo a condizione che egli possa disporne per taluni specifici scopi o in alcuni particolari contesti. S’immagini, a titolo prettamente semplificativo, che Alice sia intenzionata a donare a Bob una parte della propria disponibilità di

criptoasset, ma solo perché Bob, a propria volta, la investa in un'iniziativa di beneficienza di cui Dan ed Erin sono responsabili. Con uno script speciale agganciato alla transazione, Alice può impedire a Bob di usare la quantità di criptoasset trasferita al di fuori di un perimetro di distribuzione limitato ai soli Erin e Dan. Anche in questo caso, come per il precedente, Bob potrebbe essere in grado di ricevere i bitcoin da Alice correttamente, ma non potrebbe a propria volta disporne liberamente, ossia non potrebbe "spenderli" scambiandoli con altri all'infuori di Erin e Dan.

Uno script che trasferisce criptoasset a più destinatari contemporaneamente

Supponiamo che Alice decida di trasferire la disponibilità di parte dei propri criptoasset (ossia i bitcoin) verso Bob e Charlie, perché Charlie è in grado di soddisfare un suo bisogno e Bob è l'amico che l'ha informata della possibilità di trovare in Charlie la risposta alle sue necessità. S'immagini, a titolo prettamente semplificativo, che Alice abbia bisogno di una traduzione dal francese al giapponese; Bob conosce

il giapponese ma non sa tradurre dal francese perché è nato a Nagasaki e non è mai stato in Francia. Bob, però, sa che l'amico Charlie, anch'esso di origine nipponica, ha vissuto la sua infanzia a Nizza e, quindi, conosce la lingua francese ed è in grado di tradurla nella propria lingua madre. Per questo servizio di "informazione" Alice è disposta a corrispondere a Bob una percentuale in criptoasset della cifra pattuita con Charlie per la traduzione.

Con uno script speciale agganciato a una sola transazione, Alice può contemporaneamente trasferire sia a Charlie sia a Bob la quantità di criptoasset definita e calcolata. Volendo estendere l'uso degli script sin qui

appreso, Alice potrebbe decidere di rendere effettiva la disponibilità di criptoasset trasferita a Charlie solo se viene soddisfatta una condizione, per esempio a patto che Bob certifichi che il testo tradotto in giapponese da Charlie sia intellegibile (attenzione, Bob non conosce il francese però è in grado di confermare ad Alice che il prodotto di Charlie è effettivamente un testo scritto in giapponese).

In questo caso la disponibilità di criptoasset trasferita da Alice a Charlie si sblocca (ossia Charlie può disporne liberamente) solo a fronte di una prova rilasciata da Bob. Questo caso d'uso, in realtà, è più facilmente gestibile se, al

posto di uno semplice script, si utilizza uno “Smart Contract” (o “Distributed Contract”), scrivendo il microcodice con uno specifico linguaggio e appoggiandosi su alcuni particolari blockchain tipo Ethereum, di cui parleremo nella Parte III e nella Parte IV del libro.

12

Pregi e difetti della Blockchain

Riprendiamo ora quanto avevamo anticipato nel precedente paragrafo "L'analisi SWOT per la fase 3 (Shared Distributed Ledger)" (Capitolo 8) e concentriamoci su quegli aspetti dell'analisi che volutamente avevamo atteso a proporvi.

Ora che siamo pervenuti a una migliore contezza della Blockchain, possiamo procedere – fuori dalla metafora Welthyland – e analizzare pregi e difetti di un sistema basato su Distributed Ledger gestito dal protocollo dei Bitcoin[53].

Un impiego virtuoso della Blockchain

Tracciabilità, immutabilità e sicurezza sono le caratteristiche principali che connotano la Blockchain. Più in generale possiamo dire che sulla Blockchain dei Bitcoin è possibile individuare un sistema tale da permette di stabilire

relazioni fiduciarie tra soggetti che non si conoscono, riducendo drasticamente le vulnerabilità tipiche di un sistema che prevede un'entità centrale o un intermediario terzo. Può avere molto senso sfruttare una siffatta tecnologia, che riesce a riprodurre il concetto di scarsità nel mondo digitale, per offrire prove incontrovertibili dell'avvenuta transazione di un bene fisico ma anche di un bene immateriale[54].

Tra le opportunità di sviluppo che questa tecnologia può indirizzare vi è sicuramente quella legata all'identità, qui intesa non come una soluzione candidabile a essere implementata su Blockchain, di cui parleremo nel novero

degli ambiti applicativi cross-industry nella Parte IV di questo libro, bensì come possibilità di migliorare il processo di identificazione dei propri utilizzatori.

Nella Blockchain pubblica dei Bitcoin, l'accesso al network e la possibilità di scrivere e leggere il ledger distribuito non avvengono identificando e verificando (né previamente né mai) il soggetto possessore del wallet. In altre parole, Alice e Bob sono unicamente referenziabili mediante le loro rispettive chiavi pubbliche, ma non hanno alcuna possibilità di garantire ciò che asseriscono di essere.

Non vi è dunque un'autorità centrale

che può autenticare l'accesso alla Blockchain. Uno sviluppo estremamente interessante può essere rappresentato dall'opportunità offerta agli Identity Provider[55] di rilasciare delle credenziali che consentono di accedere al wallet, in modo tale che la generazione delle chiavi pubbliche in esso riprodotte sia riconducibile a un soggetto opportunamente identificato. Ciò non significa individuare nell'Identity Provider il ruolo svolto da Trent nella metafora di Welthyland (la validazione delle transazioni si baserebbe sempre su un sistema di consenso distribuito), bensì consentire di deanonimizzare gli accessi al

network[56].

I rischi di utilizzare una Blockchain

Privacy vs totale anonimato

Tutte le transazioni sulla Blockchain avvengono in chiaro e per ciascuna di esse rimane una traccia immutabile della loro storia: ciò significa che esiste un concreto rischio per la privacy, di fronte al quale è necessario provvedere con soluzioni che, a oggi ancora *in fieri*, prevedono di crittografare i dati delle transazioni.

Tali soluzioni propongono però

nuovi problemi dipesi essenzialmente da due fattori:

- degrado delle performance, dipeso dal carico che si introduce con la crittografia;
- totale anonimato[57].

Scalabilità, costi e rischio di concentrazione

Sulla Blockchain dei Bitcoin abbiamo detto che durante il processo di mining vengono "coniate" nuove unità di criptovaluta come sistema di

remunerazione che ripaga – almeno in parte – il costo sostenuto dai nodi validatori (risorse di calcolo, energetiche ecc.). Il modello d'incentivazione basato sulle Proof-of-Work assicura che questi ultimi vengano premiati per il loro lavoro di approvazione solo laddove il compito sia stato svolto correttamente (ossia verificato dagli altri nodi), rendendo antieconomico qualsiasi tentativo di alterazione surrettizia dei blocchi precedentemente validati. Cionondimeno, abbiamo spiegato come esista un ulteriore modello di incentivazione basato sulle commissioni (o mance, come descritte nel paragrafo del Capitolo 6 "Gli incentivi per i

validatori delle transazioni su un registro distribuito") che permette ai miner di essere ulteriormente ricompensati, in aggiunta al reward previsto per chi presenta per primo la PoW. I nodi validatori, soprattutto nei periodi di intenso traffico transazionale, tendono a scegliere i blocchi che contengono mance più significative, creando una disparità di trattamento per quegli utenti che, non volendo spendere in commissioni esorbitanti, sono costretti ad attendere ben più di un'ora per vedersi confermate le proprie transazioni. La dimensione di un blocco della Blockchain non può superare 1 MB, pertanto i miner sceglieranno di

inserire nei blocchi che si accingono a minare le transazioni con commissioni più alte, soprattutto nei periodi in cui sul network viene propagato un numero di transazioni particolarmente elevato; ne consegue che transazioni meno "redditizie" possono attendere ore prima che un miner scelga di inserirle nel proprio blocco. In questo paragrafo racconteremo quali sono stati i principali interventi che, nel corso del 2017, hanno animato la comunità dei principali miner, volti a trovare un sorta di ottimo paretiano tra la necessità di: rendere (più) scalabile la Blockchain; abbassare il costo delle commissioni; evitare il ricrearsi di "concentrazioni di fatto". Riteniamo utile spiegare

l'avvicendarsi di tali interventi, poiché essi rappresentano un *vulnus* che deve essere noto e gestito laddove si pensa di impiegare una Blockchain per finalità che, come vedremo in seguito, vanno oltre il concetto di mero scambio di criptoasset. Tali criticità minano, nella sostanza, il principio di governance condivisa tipica della Blockchain dei Bitcoin.

Bitcoin Gold

La capacità computazionale dei miner può tendere a concentrarsi nei cosiddetti "mining pool", ossia gruppi di server particolarmente costosi che sono installati e operativi in quei Paesi dove,

sfruttando il basso costo dell'energia elettrica, è possibile detenere una potenza di calcolo maggiore. Una concentrazione siffatta mette fuori gara chi non ha a disposizione elevate risorse per competere. Esiste dunque un possibile rischio che tale concentrazione conferisca un potere eccessivo a un gruppo limitato di nodi, insidiando il principio di base della Blockchain, ossia la decentralizzazione dei controlli basata su un modello di governance distribuita.

Nel tentativo di combattere questo rischio, nel mese di ottobre 2017 è nato un nuovo protocollo per la Blockchain chiamato Bitcoin Gold, che dovrebbe

rendere sostanzialmente ininfluente l'hardware – molto costoso e, perciò, disponibile solo a pochi che possono permettersene l'acquisto – basato su microprocessori ASIC (Application Specific Integrated Circuit) con cui è, oggi, possibile validare le transazioni di Bitcoin a una velocità maggiore, conferendo nuovamente la possibilità di fare mining anche a coloro che possiedono apparati meno potenti e più economici; si mitiga così il rischio di concentrazione succitato.

SegWit2X

Al fine di migliorare l'utilizzo e la scalabilità dell'infrastruttura

decentralizzata che gestisce gli scambi di bitcoin proprio laddove, in particolare nei periodi di utilizzo intensivo, il calo prestazionale è avvertito maggiormente, un gruppo di miner ha proposto nel corso del 2017 una serie di modifiche strutturali alla Blockchain, suddivise in due fasi: la prima, chiamata "Segregated Witness", prevedeva di efficientare il protocollo riducendo la dimensione delle transazioni, mediante la segregazione di alcuni metadati che accompagnano le transazioni. Tali metadati avrebbero potuto essere gestiti "off-chain", ossia al di fuori della catena. In tal modo, mantenendo la stessa dimensione del blocco originaria, ci sarebbero state più

transazioni validate nell'arco di 10 minuti, il tempo che (lo ricordiamo) è mediamente necessario per generare un nuovo blocco e aggiungerlo alla catena, per cui, in pratica, la gestione delle transazioni in Bitcoin sulla Blockchain è limitata a 6 o 7 al secondo.

Il secondo step (attivabile ove si fosse raggiunto il consenso richiesto) avrebbe dovuto condurre all'aumento della dimensione massima dei blocchi. Tecnicamente quanto avvenuto è stato non riuscire ad attivare la seconda parte di SegWit2x (ossia quella su cui maggiormente la comunità si era divisa), che avrebbe dovuto raddoppiare la dimensione dei blocchi portandoli a 2

MB, volendo con ciò incrementare l'efficienza del protocollo e, almeno in teoria, portare a una diminuzione delle commissioni richieste dai miner per validare più velocemente le transazioni.

I Bitcoin Cash

SegWit, la prima parte, con cui si era iniziato ai primi di agosto 2017, è avvenuta al netto di un compromesso che ha prodotto l'Hard Fork dei Bitcoin Cash, una nuova catena dalla quale si è originata un'altra criptovaluta (il BCH), separata dalla quella core e irreversibile, dove i blocchi hanno la dimensione massima di 8 MB. Per questa nuova blockchain, i sostenitori

hanno sempre dichiarato che avrebbe potuto costituire un buon mezzo per effettuare pagamenti P2P, attese le prestazioni decisamente superiori rispetto alla Blockchain parent.

Le Fork sulla Blockchain

Bitcoin Cash e Bitcoin Gold sono il prodotto di ciò che sulle blockchain pubbliche, basate su sistemi Distributed Ledger, si chiama “Fork” (o biforcazioni). Le Fork sono strumenti utilizzati dal network per migliorare le performance della Blockchain e per

gestire il protocollo. Si dividono in Soft Fork e Hard Fork.

Soft Fork

La Soft Fork si realizza e si attua dando vita a una versione aggiornata del protocollo compatibile con le versioni precedenti. La Soft Fork mette in atto un cambiamento reversibile che consente la partecipazione alla Blockchain anche a tutti quei nodi che, per ragioni diverse, decidono di non effettuare l'aggiornamento.

Hard Fork

L'Hard Fork prevede invece un

cambiamento irreversibile e impone ai nodi di effettuare obbligatoriamente l'aggiornamento. Con le Hard Fork vengono create nuove criptovalute, come nei casi di Bitcoin Cash e Bitcoin Gold (o prima ancora Litecoin) spiegati in precedenza.

Hard Fork Planned o Contentious

Le Hard Fork possono essere di tipo "Planned", ovvero pianificate e programmate, o di tipo "Contentious", ovvero che non riescono a trovare il consenso della comunità. In questa seconda tipologia di Hard Fork il

cambiamento proposto al protocollo non trova un accordo all'interno della comunità e si arriva, pertanto, a una forma di scissione della Blockchain. Nel caso di Hard Fork Planned il cambiamento del protocollo è pianificato e il passaggio viene approvato dai partecipanti ove sia raggiunto un *quorum* definito in fase di proposta dei cambiamenti delle regole. L'Hard Fork Planned non conduce allo sdoppiamento della catena e le regole vengono aggiornate in continuità.

Il bisogno di arrivare a una Fork

Per spiegare le motivazioni che inducono a creare le scissioni provocate dalle Hard Fork è necessario soffermarsi sul significato che il valore del criptoasset rappresenta per una Blockchain. Se si guarda al solo aspetto di riserva di valore (come abbiamo spiegato al paragrafo "Definizione di moneta" nel Capitolo 2) e intendiamo il criptoasset come una rappresentazione digitale di detto valore (in linea con ciò che presentavamo nel paragrafo "Definizione di criptoasset" del Capitolo 2) prescindendo dalla disamina di logiche speculative, comunque sempre presenti nei mercati, è importante comprendere come alcune

elementari nozioni debbano essere prese in considerazione.

Chiediamoci, innanzitutto, se sia lecito domandarsi quale possa essere il Fair Value del Bitcoin, o meglio, di quali valori si componga. Valore come riserva di valore e valore intrinseco come mezzo di scambio sono, probabilmente, gli elementi più corretti da analizzare. Partiamo dal primo. La volatilità del Bitcoin, se posta in relazione al più tradizionale bene rifugio, ossia l'oro, rende gli investimenti in questa criptovaluta assai più rischiosi. Oggigiorno, tuttavia, complice l'instabilità politica di importanti Stati sovrani e la crisi, spesso di natura altrettanto geopolitica,

di molte economie sviluppate, le comunità sono state indotte alla ricerca di altri possibili "beni rifugio".

Garrick Hileman, studioso del Centre for Alternative Finance dell'Università di Cambridge, ha recentemente asserito che potrebbe essere attribuibile al Bitcoin la definizione di "oro virtuale", un bene prezioso che si può scambiare con altri trader su mercati OTC, ma che è difficile da usare nelle spese di tutti i giorni per la lentezza intrinseca nelle transazioni.

E qui veniamo alla seconda componente del Fair Value della criptovaluta: il valore come mezzo di

scambio, ossia il valore del Bitcoin intrinsecamente legato alla possibilità (o opportunità) di essere impiegato come mezzo di trasferimento della moneta. Le prestazioni dei Bitcoin non sono all'altezza dell'utilizzo – comune – che ne fanno gli utenti, costretti ad aspettare tempi decisamente lunghi per vedere le proprie transazioni confermate, oppure a vedersi aumentare le commissioni per dare la precedenza alle proprie transazioni. L'enorme successo che ha avuto il Bitcoin ha evidenziato un problema di efficienza tipico del protocollo Blockchain e la rete si è saturata.

Perché si arriva alla Fork

Poiché la governance della Blockchain che abbiamo esaminato è basata su un modello condiviso, non esistendo un unico decisore centralizzato in grado di determinare risoluzioni, quando si vogliono cambiare le regole è necessario che la rete stessa sia d'accordo. Ed è proprio nel solco di tale determinazione che è possibile inserire l'avvicendarsi di Hard Fork quali quelle dianzi descritte.

I rischi che comportano le Hard Fork

Nei casi di Hard Fork, o meglio, durante

il propagarsi degli effetti sul network di una Hard Fork, emergono alcuni rischi che pongono in pericolo l'affidabilità e, soprattutto, l'immutabilità delle transazioni avvenute. Ciò che infatti può accadere è il manifestarsi dei cosiddetti "replay attack", dove soggetti malintenzionati replicano le transazioni sulla nuova catena appena effettuate sulla catena di origine. Tale situazione si verifica per via del fatto che i due criptoasset (quello legacy e quella della forked chain), nel periodo in cui si sta consumando la scissione, possono essere "sbloccati"[58] con la stessa chiave privata, esponendo quindi le transazioni al rischio di essere duplicate.

I *vulnus* della e-democracy

Alcune vulnerabilità tipiche delle blockchain pubbliche, ossia quelle il cui accesso segue una logica "permissionless", emergono durante il propagarsi sul network delle Hard Fork. I casi di Hard Fork che producono scissioni irreversibili della catena, con la conseguente nascita di nuove criptovalute, non sono in sé deprecabili, poiché rappresentano un metodo per esprimere miglioramenti (almeno così si auspica) in cui la comunità di sviluppatori e di miner crede. La presenza di un modello di

governance condiviso (o, se si preferisce, l'assenza di un modello di governo centrale) può rappresentare l'espressione democratica di un sistema decisionale, dove una pluralità di soggetti può esprimere il proprio voto per il conseguimento di obiettivi condivisi: una sorta di e-democracy[59]. Tuttavia, l'esercizio stesso di tale democrazia impone la necessità di prevedere, in molti casi, scissioni interne al sistema; è proprio in queste circostanze che, come nella vita materiale organizzata da una politica intesa quale espressione di una sovranità popolare, si indeboliscono le difese e si sguarnisce il fianco, esponendo l'intera comunità a rischi che devono sapersi mitigare, agendo preventivamente laddove possibile.

53. In questo caso volutamente utilizziamo l'iniziale "B" maiuscola, a voler riferire che stiamo parlando del protocollo – descritto nei precedenti paragrafi – per la Blockchain dei Bitcoin.

54. Come anticipavamo nel paragrafo "Il legame dell'asset nativo con il mondo degli scambi in un'economia reale" (Capitolo 7), in tutti questi casi è però necessario che il valore del criptoasset sia tradable, ossia possa esprimere una forma di valore riconosciuto dalla comunità più ampia in cui il trading avviene.

55. In Europa gli Identity Provider sono entità autorizzate ai sensi del Regolamento (UE) n. 910/2014 (c.d. regolamento eIDAS) a rilasciare un'identità digitale interoperabile a livello comunitario; in Italia è in vigore lo SPID (Sistema Pubblico di Identità Digitale) e

gli Identity Provider sono soggetti privati autorizzati dall'AgID (Agenzia per l'Italia Digitale). Il rilascio di un'identità digitale conforme al regolamento eIDAS prevede una fase di identificazione e verifica del cittadino a espletamento della quale vengono rilasciate le credenziali che gli consentono di accedere ai diversi servizi erogati sul territorio dell'Unione.

56. Nella Parte III del libro tratteremo espressamente di questa opportunità quando spiegheremo il significato di "permissionless ledger".

57. Seppure il dato transazionale scritto sulla Blockchain sia sempre tracciabile, laddove questi non fosse in chiaro, verrebbe vanificata qualsiasi ricerca tesa a ricondurre alla fonte originatrice della transazione. In alcuni casi si avrebbe il paradosso di poter risalire all'Address mittente (quando anche gli Address

non fossero offuscati) ma senza aver contezza di ciò che sia stato transato effettivamente.

58. Si veda al riguardo quanto spiegato al paragrafo "La struttura di un Input di transazione" nel Capitolo 10.

59. Con e-democracy si intende l'utilizzo delle tecnologie dell'informazione e della comunicazione atto a favorire la partecipazione dei cittadini alla vita democratica. In questo contesto si è ritenuto utile riferirsi a tale termine per rappresentare l'espressione democratica del sistema decisionale tipico della Blockchain.

13

I diversi protocolli del consenso distribuito

Sino a ora vi abbiamo spiegato come funziona il meccanismo che consente di gestire un consenso distribuito sulla Blockchain dei Bitcoin: la Proof-of-Work. Tale sistema non è però l'unico.

Esistono infatti diversi protocolli implementati su altre blockchain che, almeno in teoria, cercano di superare i limiti della PoW. Come abbiamo detto, le criticità di questo sistema di mining risiedono essenzialmente:

- nella velocità di validazione di un blocco; la PoW è un sistema che, al crescere della Blockchain, richiede sempre maggiore potenza elaborativa nei server dei miner (il tempo di validazione di una transazione di circa 10 minuti è una delle principali ragioni alla base delle maggiori criticità in termini di

scalabilità);

- nella possibilità di riproduzione di meccanismi di concentrazione *de facto*, con la creazione di enormi server farm che centralizzano la funzione di mining gestiti da mining pool.

Proof-of-Stake (PoS)

Mentre la PoW si basa solo sulla capacità di calcolo dei nodi validatori, la Proof-of-Stake (o "PoS") si basa sulla quota effettiva di criptoasset nella disponibilità del miner. Quindi, in un sistema PoS, più quote di criptoasset si

hanno nella rete, più si possono validare i blocchi. Per esempio, se un miner detiene una quota del 5% del totale della criptovaluta in circolazione, tale miner può validare solo il 5% dei blocchi.

In termini di sicurezza, attaccare la rete richiederebbe all'attaccante di possedere quote di criptovaluta maggioritarie. Tuttavia, per il principio che abbiamo più volte ribadito in merito al valore di trading attribuito dalla comunità al cripto-asset, più l'attaccante acquistasse criptovaluta più il prezzo della medesima potrebbe aumentare (in definitiva vale la legge del mercato). Quando l'autore dell'attacco dovesse riuscire ad avere sufficiente disponibilità di criptoasset per attaccare

il network e imporre la propria verità sulle transazioni validate (una verità fallace o mendace, ovviamente), l'attacco sarebbe per sé stesso controproducente in quanto interesserebbe (ovvero colpirebbe) proprio colui che dispone della maggior parte di criptoasset in circolazione, ossia il miner disonesto attaccante. Invece, laddove competesse secondo le regole corrette, la PoS potrebbe realmente consentirgli quella giusta remunerazione per l'attività di validazione effettuata.

Il protocollo prevede inoltre che quando viene agganciato un nuovo blocco alla catena venga

automaticamente scelto il creatore del blocco successivo[60]. Per effettuare questa selezione vengono a oggi utilizzati metodi diversi[61]:

- **Peercoin** effettua una selezione casuale abbinandola al concetto di anzianità, ossia il numero di giorni che il miner scelto deve dimostrare di avere in termini di disponibilità del criptoasset (il cosiddetto "tempomoneta").
- **Reddcoin** utilizza un algoritmo basato sulla velocità delle transazioni[62] al fine di esortare la movimentazione di criptovaluta piuttosto che il suo

possesso (il miner che accumulasse soltanto verrebbe penalizzato).

- **BlackCoin** si basa su una funzione casuale randomizzata con una formula che cerca il valore di Hash più basso rapportato alla dimensione della somma in gioco.

Il sistema basato su Proof-of-Stake è attuabile su blockchain pubbliche, dove l'accesso al Distributed Ledger è di tipo permissionless (come la Blockchain dei Bitcoin); tuttavia, rispetto a un sistema basato su PoW è molto meno costoso in termini di consumo di energia.

La Proof-of-Stake "Casper" proposta per Ethereum

La blockchain di Ethereum è basata, al momento in cui scriviamo questo libro, su un'architettura Distributed Ledger di tipo permissionless[63], dove vige un protocollo per il consenso distribuito costruito su PoW.

Da qualche mese è stato proposto un aggiornamento chiamato "Casper", presentato come metodo maggiormente efficiente per validare i blocchi. Piuttosto che passare drasticamente da un sistema Proof-of-Work a un sistema

Proof-of-Stake, dovrebbe avvenire un cambio più graduale mediante l'applicazione di un algoritmo ibrido PoW/PoS. Il sistema PoW verrà adottato per validare la maggioranza dei blocchi Ethereum, mentre il sistema basato su PoS sarà impiegato come meccanismo di "checkpoint" a ogni 100 blocchi.

Proof-of-Authority (PoA)

Il sistema Proof-of-Stake elimina la necessità di spendere una quantità enorme di energia elettrica per convalidare i blocchi, rispetto al sistema PoW. L'assunto che supporta la Proof-

of-Stake è il seguente: i nodi validatori che detengono una maggiore partecipazione nel network (sempre espressa in termini di maggiore disponibilità di criptoasset) sono incentivati ad agire nel proprio interesse. A parità di tutti gli altri, più la quota di partecipazione è consistente, più alto dovrebbe essere l'interesse del miner nel preservare il sistema. Questo sistema, tuttavia, rischia di essere meno efficace quando un miner possiede una quota di criptoasset nettamente inferiore, in termini relativi, rispetto ad altri, per esempio perché è entrato a far parte della comunità in tempi più recenti. Il miner più "giovane" (ossia quello con minore disponibilità di criptovaluta)

potrebbe essere meno incentivato, in una proporzione pari alla differenza che emerge dal confronto con il miner più "ricco".

Il sistema basato su Proof-of-Authority rappresenta invece un meccanismo di consenso alternativo in cui i nodi che convalidano i blocchi sono solo quelli esplicitamente autorizzati, con una modalità simile a quella descritta nel precedente paragrafo "Un impiego virtuoso della Blockchain" (Capitolo 12). Con una corretta adozione della PoA, invece di puntare solo sul valore della quota di criptovaluta posseduta, si considera anche l'identità di un validatore. In

questo contesto per “identità del validatore” si intende un’identità che sia stata effettivamente verificata da un soggetto terzo, previa verifica della corrispondenza tra l’identificazione personale del miner con la documentazione ufficialmente rilasciata per la stessa persona; ciò equivale ad assumere che un nodo validatore sia esattamente chi dice di essere. L’uso di un protocollo per il consenso distribuito basato su PoA potrebbe essere particolarmente utile in quei contesti che descriveremo nella Parte III di questo libro, quando tratteremo dei modelli “ibridi” di blockchain.

Il problema dei generali bizantini

La metafora dei generali bizantini è utilizzata nei sistemi informatici distribuiti ogni volta che si ha la necessità di determinare una votazione il cui risultato può essere o vero o falso e quando si rende necessario efficientare il più possibile il lavoro di determinazione del voto stesso. Questo scenario può rappresentare il problema tipico del consenso distribuito su una blockchain, dove si cerca di individuare un protocollo alternativo alla Proof-of-Work e alla Proof-of-Stake al fine di risparmiare

energia, avendo comunque la certezza di raggiungere un'unica versione di verità verso la quale converge una maggioranza di consensi.

Il problema: ci sono alcuni generali (in numero dispari) dell'Impero Bizantino che stanno accerchiando la città di Roma, ognuno con il proprio esercito. Per espugnare la città i generali devono decidere se attaccare o ritirarsi. La situazione a contorno impone che i generali possano comunicare solo tramite messaggeri e che sia impedito loro di riunirsi; inoltre si è a conoscenza dell'esistenza di alcuni traditori infiltratisi nel gruppo, ma non se ne conosce l'identità e neppure il numero. L'assedio avrà successo se i generali leali riescono a trovare un accordo sulla loro strategia.

Fuor di metafora, il consenso sulla blockchain viene raggiunto quando vi è un rapporto tra miner "buoni" e miner "disonesti" predeterminato, la cui validazione è risolta dall'algoritmo di derivazione BFT, ossia Byzantine Fault Tolerance.

Proof-of-Elapsed-Time (PoET)

Uno dei più interessanti algoritmi su cui si basano alcuni protocolli del consenso distribuito (per esempio quello di Hyperledger Sawtooth che vedremo più avanti) è la Proof-of-Elapsed-Time (PoET). Ogni partecipante al network

può assurgere al ruolo di nodo validatore delle transazioni richiedendolo, in sicurezza, mediante specifiche funzioni descritte nelle regole del protocollo. In un determinato istante potranno aversi diversi partecipanti che provano a domandare l'ottenimento di tale privilegio; il vincitore, ossia colui che sarà eletto "leader" e avrà la possibilità di minare le transazioni, sarà chi avrà speso il tempo minore di attesa, assegnato in modo casuale dal sistema. Trascorso questo periodo, un'ulteriore funzione controllerà che il leader abbia conseguito in modo legittimo la possibilità di validare i blocchi, ossia autenticandosi con successo, e solo laddove ciò sia verificato sarà

riconosciuto tale dalla comunità. La probabilità di essere eletto è direttamente proporzionale al livello di contribuzione elargita a sostegno del network, misurando il contributo sulla quantità di risorse computazionali generiche rese a disposizione[64].

Il sistema PoET è in termini energetici evidentemente meno pretenzioso rispetto al PoW dei Bitcoin, pur garantendo un buon livello di sicurezza, sempre basato sul concetto di fiducia distribuita. Inoltre, l'esiguità dell'investimento richiesto per partecipare al network è tale da incentivare anche i piccoli utilizzatori a partecipare seguendo le regole di questo

protocollo del consenso.

L'utilizzo di PoET all'interno di blockchain "Hybrid" o "Private"[65], dove i partecipanti sono – di norma – società o comunque persone giuridiche non semplici (si pensi a un raggruppamento di imprese consorziate, per esempio), diviene particolarmente efficace nel perseguimento di obiettivi di disincentivazione dei comportamenti illeciti, avendo *in primis* gli stessi partecipanti tutto l'interesse a rimanere nel gruppo. Un partecipante che agisse disonestamente sarebbe emarginato dalla comunità e patirebbe l'esclusione in quanto antieconomica per sé stesso.

Il “giusto mezzo” della PoET

Un protocollo di consenso distribuito che si basa sulla Proof-of-Elapsed-Time potrebbe candidarsi a rappresentare un buon compromesso tra le esigenze di scalabilità e fiducia distribuita sulla blockchain perché garantirebbe:

- **un giusto investimento**, dato che i costi per diventare miner potrebbero essere direttamente

proporzionali ai vantaggi che ne discendono;

- **ampiezza del consenso distribuito**, in quanto a chiunque potrebbe essere consentito validare un blocco in un contesto il più ampio possibile;
- **facilità di verifica** per tutti i partecipanti, che potrebbero appurare la legittimità del leader in modo semplice, rapido e certo.

60. Il nodo individuabile non può essere quello che ha una posizione dominante nella catena come, per esempio, il miner che possiede la maggior quantità di criptovaluta, posto che ove così fosse sarebbe colui che potrebbe minare tutti i successivi blocchi.

61. I nomi dei sistemi che compaiono nella lista coincidono con i nomi dei criptoasset gestiti sulle rispettive blockchain che adottano il sistema PoS.

62. La variante PoS del protocollo di consenso distribuito alla base della blockchain dei Reddcoin è altresì nota con il termine PoSV (Proof of Stake Velocity).

63. Nella Parte III di questo libro, "DLT (Distributed Ledger Technology)", entreremo nel dettaglio delle diverse tipologie di Distributed Ledger e spiegheremo la blockchain di Ethereum.

64. Il fatto che i requisiti di potenza computazionale siano generici implica che eventuali computer ASIC basic progettati per eseguire efficacemente e in efficienza solo alcuni algoritmi (come abbiamo visto per la Blockchain dei Bitcoin, è il rischio che si è cercato di mitigare con la Fork dei Bitcoin Gold) siano messi automaticamente fuori gioco.

65. Spiegheremo il significato di blockchain "Hybrid" e "Private" nel Capitolo 16.

PARTE III
DLT (DISTRIBUTED LEDGER TECHNOLOGY)

La tecnologia è al suo meglio quando è invisibile.

Nassim Nicholas Taleb

14

Non solo Bitcoin

Dopo avervi spiegato in un dettaglio ragionevolmente profondo cosa sia la Blockchain dei Bitcoin, in questa terza parte del libro affronteremo il più ampio tema delle blockchain (con la “b” iniziale minuscola), ossia di quelle piattaforme basate su una tecnologia che gestisce l’accesso e la scrittura di un ledger distribuito, non finalizzato a

consentire gli scambi della più famosa criptovaluta.

Riprenderemo in esame il concetto proposto nell'Introduzione del libro, quando abbiamo definito la blockchain come l'**Internet del Valore**, nozione che d'ora in avanti assumeremo trasversale in ogni contesto che andremo ad analizzare.

La Internet of Value su blockchain

La Internet of Value è una rete digitale di nodi che si trasferiscono valore, anche in assenza di fiducia, attraverso un sistema di algoritmi e regole criptografiche che permette di raggiungere il consenso sulle modifiche di un registro distribuito che tiene traccia dei trasferimenti di valore tramite asset digitali univoci.

Nella Figura 14.1 riportiamo una panoramica offerta dall'Osservatorio su Blockchain e Distributed Ledger del Politecnico di Milano, con la quale si dà evidenza di come si possano mappare i termini essenziali che definiscono la Internet of Value sulle diverse blockchain.

Figura 14.1 – Mappatura della definizione di Internet of Value su blockchain.

Le principali blockchain

Andiamo ora a descrivere le principali blockchain alternative a quella dei Bitcoin, soffermandoci in particolare sull'architettura che sottende a Ethereum.

Ethereum

Che cos'è Ethereum

Ethereum potrebbe essere presentato come il più grande computer condiviso che è in grado di erogare una enorme potenza disponibile ovunque e per sempre.

Secondo il sito ufficiale[66] "Ethereum è una piattaforma decentralizzata che gestisce "contratti intelligenti" o "Smart Contract"[67]. Dunque, con Ethereum si passa dal concetto di database distribuito che abbiamo assunto per spiegare la Blockchain dei Bitcoin al concetto di "Distributed Computing". La diversità si esprime nella capacità di

consentire la creazione di microcodice molto simile a quello descritto per gli script della Blockchain nel Capitolo 11 ma molto più potente, al punto da potergli conferire a pieno diritto l'appellativo di "moneta altamente programmabile", sulla falsariga di quanto avevamo anticipato con la spiegazione dello script al paragrafo "Uno script che trasferisce criptoasset a più destinatari contemporaneamente" (Capitolo 11) illustrando lo use case più complesso. Ethereum è progettata per essere una piattaforma programmabile capace di dare vita a diverse tipologie di applicazioni decentralizzate non necessariamente limitate alla sola gestione delle transazioni in

criptovaluta.

Ether e Gas: la moneta di scambio e il "carburante" di Ethereum

L'uso delle risorse computazionali di Ethereum è remunerato con una speciale criptovaluta denominata "Ether".

Qualsiasi transazione per essere eseguita ha bisogno di una certa quantità di "Gas". Ciò impedisce l'attuazione di un ciclo di contratti infinito, poiché l'esecuzione termina una volta che il

Gas si esaurisce. Questo Gas può essere acquistato in cambio di Ether. I prezzi del Gas sono piuttosto bassi e vengono acquistati in Wei al seguente rapporto di cambio:

- 1 Ether = 10^{-10} Wei

Il prezzo del Gas è variabile ed è regolato dalla legge della domanda e dell'offerta sulla blockchain di Ethereum. Vediamo un esempio di transazione su Ethereum e calcoliamone il costo:

- Alice trasferisce una quantità X di Ether a Bob;
- Alice invierà a Bob "X + prezzo del Gas di default";

dove il prezzo del Gas di default è determinato da una serie di condizioni e azioni che devono essere verificate e avviate nell'esecuzione della transazione, fra cui sono ricomprese la crittografia SHA-3 e la quantità di dati presenti nella transazione[68]. Tale costo di transazione può essere inteso da Alice come l'acquisto di spazio o il prezzo d'inclusione della transazione in un blocco che verrà validato da un miner. Il Gas in più rimasto dopo l'esecuzione della transazione sarà conferito al miner (una volta presentata la PoW) in aggiunta alla ricompensa, similmente a quanto può avvenire sulla Blockchain dei Bitcoin nel caso in cui vi

siano delle mance associate alle transazioni[69]. Anche in questo caso, dunque, un miner ha libertà di scelta se includere una particolare transazione nel suo blocco o meno. Quindi, più la quantità di Gas in eccesso inviata con la transazione è maggiore, maggiori sono le possibilità per la transazione di venire confermata. Non inviare abbastanza Gas con una transazione può demotivare i miner, che di certo darebbero priorità di inclusione nel blocco che si avviano a validare ad altre transazioni più "Gasate", con la conseguenza di far attendere Alice (nel nostro caso di esempio) un tempo più lungo per aver conferma della transazione a beneficio

di Bob.

Ethereum Virtual Machine EVM: il “motore” di Ethereum

Ethereum è un sistema “Turing complete” che permette agli sviluppatori di creare applicazioni che girano sulla EVM utilizzando specifici linguaggi di programmazione. Il motore di Ethereum è rappresentato dalla Ethereum Virtual Machine (EVM) che rappresenta di fatto l’ambiente di runtime per lo sviluppo e la gestione degli Smart Contract. EVM opera in modo protetto, ossia segregato

rispetto al network. Il codice gestito dalla Virtual Machine non ha accesso alla rete e gli stessi Smart Contract generati sono autonomi e indipendenti nonché separati da altri Smart Contract.

I linguaggi di programmazione impiegati su Ethereum

I linguaggi con cui sono sviluppati gli Smart Contract su Ethereum sono principalmente tre: Solidity, Serpent e LLL. Solidity è molto simile a Java e rappresenta il linguaggio più usato e supportato dalla comunità Ethereum.

Serpent è un'implementazione simile a Python e LLL è un'implementazione simile al Lisp.

Ethereum Foundation ed Ethereum Classic

Nel 2016 Ethereum è stata divisa in due diverse blockchain: Ethereum Foundation ed Ethereum Classic. Ethereum Foundation è l'organizzazione che ha come obiettivo la gestione di tutte le attività di

sviluppo, di ricerca e di supporto della piattaforma.

Ethereum Classic è il frutto di un'importante scissione nel nucleo originario di Ethereum a livello di Ethereum Foundation. In particolare, Ethereum Classic[70] è costituita dai membri Ethereum che hanno deciso di dare vita a una nuova versione di Ethereum, non condividendo le linee di sviluppo di Ethereum Foundation. Ethereum Classic è gestita da un diverso team rispetto a Ethereum Foundation ed è un network che nelle intenzioni dei suoi promotori resta pienamente compatibile con la tecnologia Ethereum, ma aggiunge una serie di servizi pensati per aumentare la sicurezza e la usabilità. Ethereum Classic è basata sullo sviluppo di una blockchain non attaccabile e ha

sviluppato una strategia di emissione dei token in proporzione allo sviluppo della rete nel corso del tempo, allo scopo di limitare i rischi di deflazione della criptovaluta.

La profonda frattura venutasi a creare sul concetto di base di una blockchain

Mentre Ethereum rappresenta la versione “ufficiale” della blockchain ed è gestita e aggiornata dagli sviluppatori che l’hanno ideata e realizzata, Ethereum

Classic è una blockchain che partendo da Ethereum si pone come una evoluzione o come una forma di alternativa.

Il motivo che ha condotto a questa divisione è legato a uno specifico evento di hackeraggio che ha colpito un famoso progetto Ethereum ("The DAO") e che ha indotto la comunità a cambiare il codice della blockchain per rimediare alle conseguenze di questo attacco. Tale decisione ha aperto una frattura molto profonda sul concetto stesso di blockchain, ovvero sui principi di fondo che reggono l'intero paradigma.

Da una parte vi sono i sostenitori che credono in un modello di e-democracy quale quello che abbiamo

raccontato nel precedente paragrafo “Le Fork sulla Blockchain” (Capitolo 12) dedicato alla disamina delle Fork e, sulla base di tale convinzione, accettano che le regole del protocollo possano essere cambiate se la maggioranza della comunità (o al raggiungimento della percentuale di consenso impostata prima di sottoporre i cambiamenti al protocollo) è d’accordo.

C’è poi una diversa scuola di pensiero che invece sostiene che le regole del protocollo non possono essere cambiate e che la blockchain deve essere saldamente protetta da qualsiasi forma di manomissione. Questa divisione ha posto gli

sviluppatori davanti a un bivio e i cosiddetti “puristi”, quando Ethereum ha creato una nuova blockchain, hanno scelto di continuare a operare sulla vecchia versione. In sostanza, con questo passaggio si sono venute a creare due blockchain Ethereum e in particolare Ethereum Classic opera oggi come versione parallela.

Ripple

Ripple è una blockchain di tipo “ibrido”[71] utilizzata per inviare denaro in tutto il mondo sfruttando le capacità di un’architettura basata sul modello Shared Decentralized Ledger (modello

adottato nella fase 2 di Welthyland, per ricordare la metafora introduttiva).

Entrando a far parte della rete globale di Ripple, le istituzioni finanziarie possono elaborare i pagamenti dei propri clienti in qualsiasi parte del mondo in modo istantaneo, affidabile ed economico. Le banche e i fornitori di pagamenti possono utilizzare l'asset digitale XRP per ridurre ulteriormente i costi e accedere a nuovi mercati[72].

Che cosa sono gli

XRP

XRP è la sigla con cui viene rappresentato l'asset nativo di Ripple; viene impiegato come una sorta di valuta di compensazione universale per semplificare le transazioni internazionali, rendendole più rapide e meno costose. Con valuta di compensazione, però, non s'intende un sistema monetario adatto a effettuare pagamenti al dettaglio. Nella sostanza, XRP potrebbe essere considerato un sistema valutario privato su cui i partecipanti, per esempio le banche, esprimono il loro consenso multilaterale dando vita a ciò che in inglese viene chiamato Automatic Clearing House (o ACH).

Una piattaforma di scambi interbancari

L'idea di base su cui si è sviluppata Ripple è stata quella di offrire una piattaforma di "scambi interbancari" che usano l'XRP come valuta di compensazione. Con XRP si può ipotizzare di creare delle nuove ACH, anche in affiancamento a quelle tradizionali. La liquidità che un asset nativo come XRP dovrebbe avere al fine di poter essere impiegato come valuta di compensazione non si crea *ex nihilo* solo basandosi su una serie di accordi

multilaterali tra soggetti interessati al suo impiego. L'apertura al pubblico potrebbe accrescere questa liquidità; tuttavia, per i privati che, differentemente da quanto abbiamo visto per la Blockchain dei Bitcoin, non possono liberamente partecipare in qualità di validatori (ricordiamoci sempre la metafora di Welthyland – fase 2, dove i Trent sono preselezionati da Grace), l'utilità intrinseca del criptoasset XRP è pressoché nulla poiché non possono usarlo sul network Ripple, a meno che non si candidino a operare come nodi validatori. In questa fase, dunque, il successo di XRP è unicamente dipeso da una logica speculativa; cionondimeno, nell'ultima

parte di questo libro dedicata alle strategie, recupereremo questi concetti rivalutandoli in una logica partecipativa istituzionale che potrebbe figurare nuovi scenari.

Il funzionamento di Ripple

Contrariamente alle blockchain di Bitcoin e di Ethereum, Ripple non richiede ai miner la resa a disposizione di una potenza computazionale per risolvere puzzle crittografici usati a titolo di Proof-of-Work per convalidare i blocchi. Il network di Ripple si basa su

uno Shared Decentralized Ledger (come abbiamo visto nella Figura 8.1), dove i nodi validatori sono preselezionati e, al momento, coincidono con le banche che hanno deciso di accordarsi tra loro per usare la blockchain. La quantità di criptoasset è già stata creata, ma solo il 40% è stata immessa sul mercato (la restante parte è bloccata) e i blocchi sono convalidati da un sistema di voto.

Hyperledger

Se fino a ora abbiamo visto modelli di blockchain in qualche misura "ispirati" alla fase 3 di Welthyland (Bitcoin ed Ethereum) o alla fase 2 (Ripple), per i

quali esistono specifici protocolli atti a gestire il consenso distribuito, dove il cripto-asset ha una propria funzione, con Hyperledger andremo a esplorare un'architettura basata su Shared Decentralized Ledger, dove non esiste un asset nativo. Classificabile come una blockchain del tipo "permissioned"[73], potremmo considerare Hyperledger alla stregua di un consorzio (similmente a quanto vedremo successivamente con Corda) aperto allo sviluppo di soluzioni innovative open source, ma destinate ad aziende private in grado di garantire alcune caratteristiche di base agli utilizzatori quali la segregazione dei dati e la privacy. L'adesione a Hyperledger

presuppone la sottoscrizione e il pagamento di quote. Nel seguito presenteremo alcune tra le più famose implementazioni su Hyperledger.

Hyperledger Fabric

Fabric è un'implementazione supportata da IBM[74] che consente agli utilizzatori di comunicare e interoperare sul network solo se in possesso di alcuni specifici permessi. Funzionalmente Fabric appare piuttosto simile a un database distribuito dove l'amministratore fornisce privilegi differenti ai diversi utenti. Pensato anche per implementare e rendere operative

particolari tipologie di Smart Contract, prevede la possibilità di realizzare delle comunicazioni "private" tra utenti (i cosiddetti "canali") preservando all'interno di essi la privatezza dei dati delle transazioni. Sebbene non disponga nativamente di un criptoasset, su Fabric può comunque essere implementato un sistema di tokenizzazione[75] e possono essere create delle criptovalute anche se, a differenza delle altre blockchain che abbiamo descritto, la loro funzione non è strettamente correlata a meccanismi di reward. I nodi validatori, infatti, operano sulla base di una preselezione, sono quindi noti *ex ante*[76], e non hanno alcuna necessità di

pervenire a un unico consenso mettendosi in gara, come abbiamo visto dover fare per i miner dei Bitcoin.

Hyperledger Sawtooth

Sawtooth è un prodotto supportato da Intel[77] che permette anche la creazione di blockchain "permissionless"[78]. Basato su un protocollo per il consenso distribuito del tipo Proof-of-Elapsed-Time (PoET)[79], con Sawtooth è possibile cambiare le regole che governano la blockchain senza la necessità (o il rischio) di avviare delle Fork, come abbiamo spiegato per

Bitcoin o Ethereum[80].

Corda

Corda è una piattaforma basata su Shared Decentralized Ledger realizzata per registrare, gestire e sincronizzare accordi tra le parti, progettata sin dall'inizio per l'impiego a uso di istituti finanziari regolamentati. Sviluppatasi nel solco del Consorzio R3, un'iniziativa intercontinentale attiva da settembre 2015 che vede la partecipazione di circa un centinaio di banche, Corda è il risultato di oltre due anni di intensa attività di ricerca e sviluppo e soddisfa i più elevati

standard del settore bancario, pur essendo applicabile a qualsiasi scenario commerciale. Anche con Corda, alla stessa stregua delle blockchain che abbiamo sin qui presentato, i partecipanti possono effettuare transazioni senza la necessità di autorità centrali.

R3

R3 nasce dall'esigenza comune di molte banche e istituti finanziari di individuare una soluzione che consentisse di superare le inefficienze

operative causate dalla difficoltà di rendere interoperabili piattaforme tecnologiche legacy, in molti casi ormai obsolete. Riconoscendo il potere della tecnologia Distributed Ledger e l'opportunità di mettere a valore gli effetti di rete tipici delle soluzioni su di essa implementate, R3 rappresenta oggi una grande realtà che cresce e si sviluppa su un modello collaborativo, partecipato da un centinaio di istituzioni finanziarie e regolatori che operano a livello intercontinentale.

Volendo riassumere in poche parole, la mission di Corda **è ridefinire le fondamenta della finanza servendosi** del potere di network collaborativi.

Le principali caratteristiche di Corda

Riassumiamo qui di seguito ciò che, con ogni probabilità, rappresenta lo spettro di specificità che distingue Corda da altre blockchain:

- **Focalizzazione sugli aspetti regolamentativi**. Corda è creata sin dall'inizio per abilitare un'autorità di regolamentazione e supervisione a operare in qualità di "nodo osservatore".
- **Implementazione degli Smart**

Contract maggiormente relazionata alla prosa legale, rispetto agli Smart Contract di Ethereum.

- **Consenso distribuito** basato su protocolli che implementano algoritmi BFT[81] (similmente a quanto abbiamo visto per Hyperledger Fabric): l'unicità dell'accordo viene raggiunto tramite l'azione di specifici nodi validatori chiamati "notary" che eseguono gli Smart Contract, avendo cura di verificare che gli input processati in un determinato momento non siano consumati

da altri partecipanti.

Anche per Corda, come per Hyperledger, la vocazione è molto orientata alla creazione di soluzioni enterprise che, tuttavia, sono progettate più specificatamente per i mercati finanziari. Sotto il profilo della privacy, similmente a quanto avviene con Hyperledger, le transazioni sono propagate solo ai nodi rilevanti.

Corda riutilizza skill di sviluppo esistenti, rendendo possibile una più rapida integrazione con i sistemi bancari pregressi. Permette l'interfacciamento e la interoperabilità con database esistenti mediante SQL e la creazione di microcodice per gli Smart Contract con

linguaggi standard come Java.

Central Bank Digital Cash – CBDC

Un progetto estremamente importante che R3 sta sviluppando sulla blockchain di Corda dovrebbe consentire alle banche centrali di emettere moneta *fiat*[82] su Distributed Ledger, al fine di abilitare un mercato FX[83] di pagamenti internazionali istantanei. In modo abbastanza simile a come abbiamo descritto nel caso di Ripple, l'obiettivo è di abilitare uno scambio diretto di CBDC (Central Bank Digital Cash)

efficientando il regolamento (settlement) dei titoli internazionali.

---

66. La piattaforma Ethereum di cui trattiamo in questo paragrafo propone il proprio sito Internet al seguente indirizzo: https://www.ethereum.org.

67. Spiegheremo nel dettaglio che cosa siano nella Parte IV del libro.

68. Tecnicamente ogni pattern di 256 bit per il quale deve essere calcolato l'Hash "costa" 6 unità di Gas.

69. Si veda quanto abbiamo spiegato al paragrafo "Mance (o commissioni)" (Capitolo 9).

70. La piattaforma Ethereum Classic propone il proprio sito Internet accessibile al seguente indirizzo https://ethereumclassic.github.io.

71. Spiegheremo il significato di blockchain ibrida nel Capitolo 16.

72. Il sito web di Ripple è accessibile al seguente indirizzo: https://ripple.com.

73. Spiegheremo il significato di blockchain "permissioned" nel Capitolo 16.

74. A luglio 2017 la Linux Foundation ha lanciato il progetto Fabric 1.0.

75. Spiegheremo il significato di tokenizzazione nel Capitolo 17.

76. Per questo motivo Hyperledger Fabric può essere rubricata alla categoria delle blockchain "private", come spiegheremo nel Capitolo 16.

77. A gennaio 2018 la Linux Foundation ha lanciato il progetto Sawtooth 1.0; nel corso del 2017 Intel aveva sviluppato una propria versione, chiamata Sawtooh Lake.

78. Spiegheremo il significato di blockchain "permissionless" nel Capitolo 16.

79. Si veda il Capitolo 13 per una spiegazione della PoET.

80. Hyperledger Sawtooth può essere rubricata alla categoria delle blockchain "Hybrid", come spiegheremo nel Capitolo 16.

81. Si veda il box "Il problema dei generali bizantini" (Capitolo 13) per una spiegazione degli algoritmi BFT.

82. Si veda il paragrafo "Definizione di moneta" (Capitolo 2) per una definizione di "moneta *fiat*".

83. Il Foreign Exchange Market, detto anche Forex (FX), o più semplicemente mercato valutario, si ha quando una valuta nazionale viene scambiata con un'altra.

16

Nella galassia delle DLT

Siamo giunti al punto in cui, forti della conoscenza che abbiamo fatto di altre tipologie di blockchain diverse da quella dei Bitcoin, possiamo chiudere questa terza parte del libro proponendo una classificazione generale delle DLT. Sappiamo che ogni blockchain si basa su

una tecnologia di registro condiviso e distribuito (DLT) che si può differenziare in funzione di alcune caratteristiche, fra cui l'accesso al network, l'identità dei miner e la presenza di un'entità terza che può preselezionare i partecipanti. In questo capitolo vi proponiamo un sistema di categorizzazione basato su:

- tipologia di ledger;
- modello di governance.

Tipologie di ledger

Le due principali categorie cui ascrivere le DLT in funzione della modalità di accesso al ledger sono descritte

puntualmente nelle successive Figure 16.1 e 16.2, nelle quali abbiamo rimarcato alcuni elementi distintivi:

1. **presenza o assenza di una terza parte "trusted"**, ossia una sorta di Grace – per ricordare la metafora di Welthyland – nella quale la comunità riconosce fiducia e dalla quale i partecipanti accettano di essere selezionati e identificati;
2. **accesso alla blockchain** (condizionabile o incondizionato);
3. **identità dei partecipanti** (nota o pseudo-anonima).

Dai primi due elementi distintivi – che rimandano a una logica di "permessi" – dipende il nome attribuito alle DLT ("permissionless" o "permission"). Il terzo elemento (l'identità) è direttamente connesso ai primi due, dipendendone funzionalmente.

Permissionless ledger

Le caratteristiche delle DLT permissionless ledger (anche chiamate "DLT permissionless" o "blockchain permissionless") sono evidenziate nella Figura 16.1.

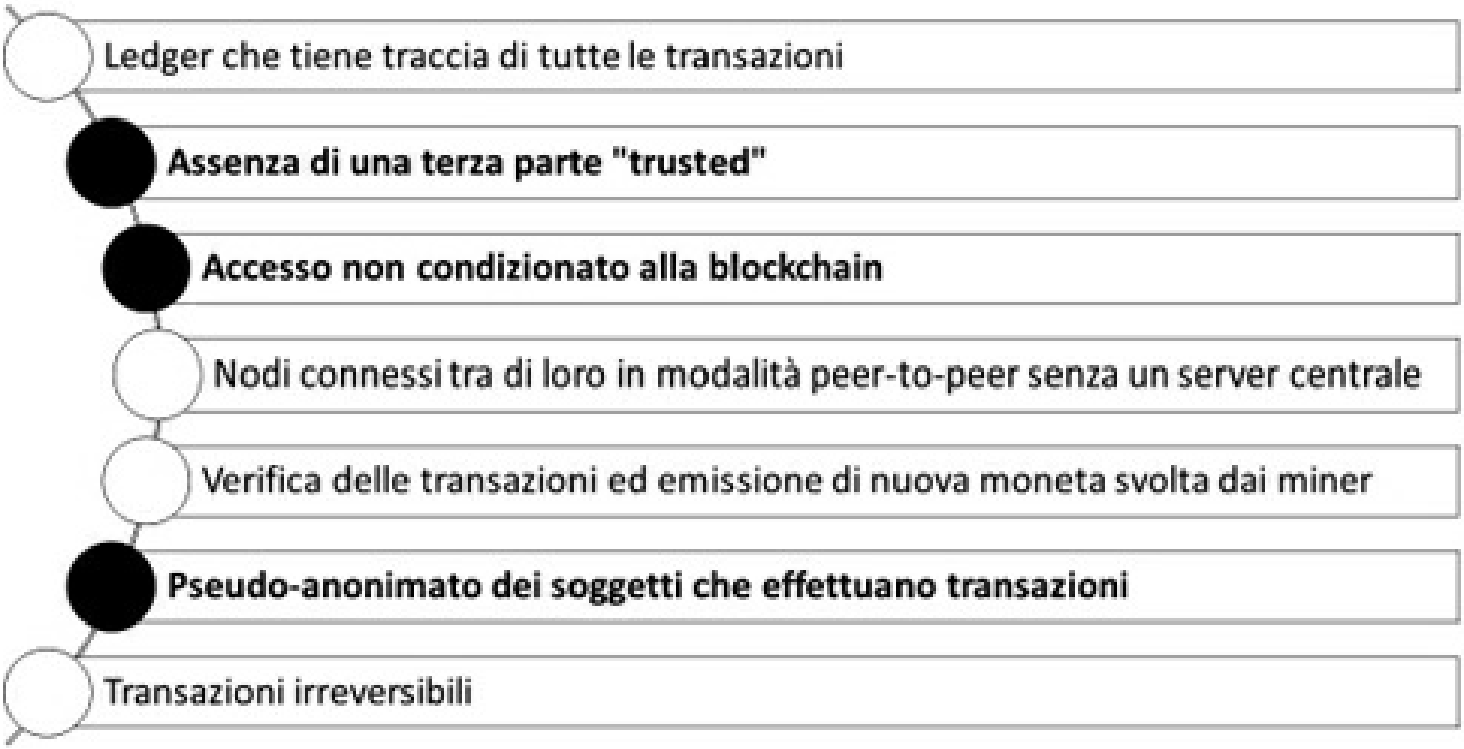

Figura 16.1 – Permissionless ledger.

In questa categoria rientrano le blockchain dei Bitcoin, di Ethereum e, in generale, quelle che si basano su un protocollo per il consenso distribuito che impiega PoW o PoS.

Permission (o permissioned) ledger

Le caratteristiche delle DLT permission ledger (anche chiamate “DLT permissioned” o “blockchain permissioned”) sono evidenziate nella Figura 16.2.

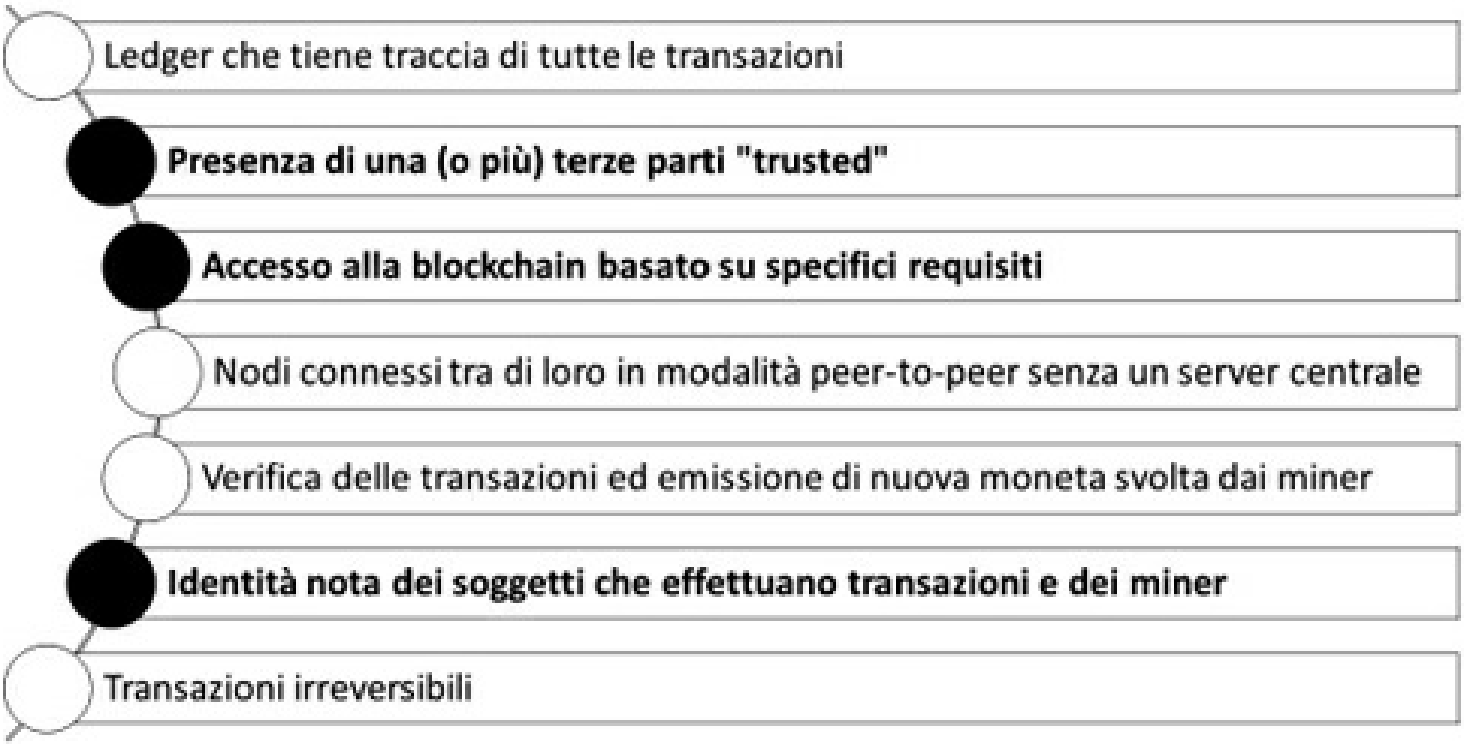

Figura 16.2 – Permission ledger.

In questa categoria rientrano blockchain come Corda, Hyperledger, Ripple e, in generale, quelle che si basano su un protocollo per il consenso distribuito che impiega un sistema BFT.

Modelli di governance

Scendendo in un ulteriore dettaglio, è possibile distinguere tre diverse tipologie di blockchain, in funzione del sistema con cui viene governata l'infrastruttura basata sull'adozione di DLT:

- **Fully Public Systems**, dove chiunque può leggere e presentare transazioni sul ledger, partecipando come membro del network alla loro verifica e convalida in qualità di miner.
- **Fully Private Systems**, dove un'entità centrale "trusted" assegna le autorizzazioni a soggetti noti che possono accedere al ledger.
- **Hybrid/Consortium Systems**, dove il processo di validazione del consenso è attuato da individui o organizzazioni, come per

esempio un consorzio di istituti finanziari clienti di un'azienda, noti e preselezionati da un'entità terza "trusted".

Seguendo questa classificazione si ha che la Blockchain dei Bitcoin (e della maggior parte delle sue Fork) e di Ethereum (pre Casper) appartiene a un modello Fully Public. La blockchain di Hyperledger Fabric è del tipo Fully Private. Le blockchain di Ripple, Hyperledger Sawtooth ed Ethereum (post Casper) si ascrivono al modello Hybrid e la blockchain di Corda potrebbe appartenere al modello Consortium (Figura 16.3).

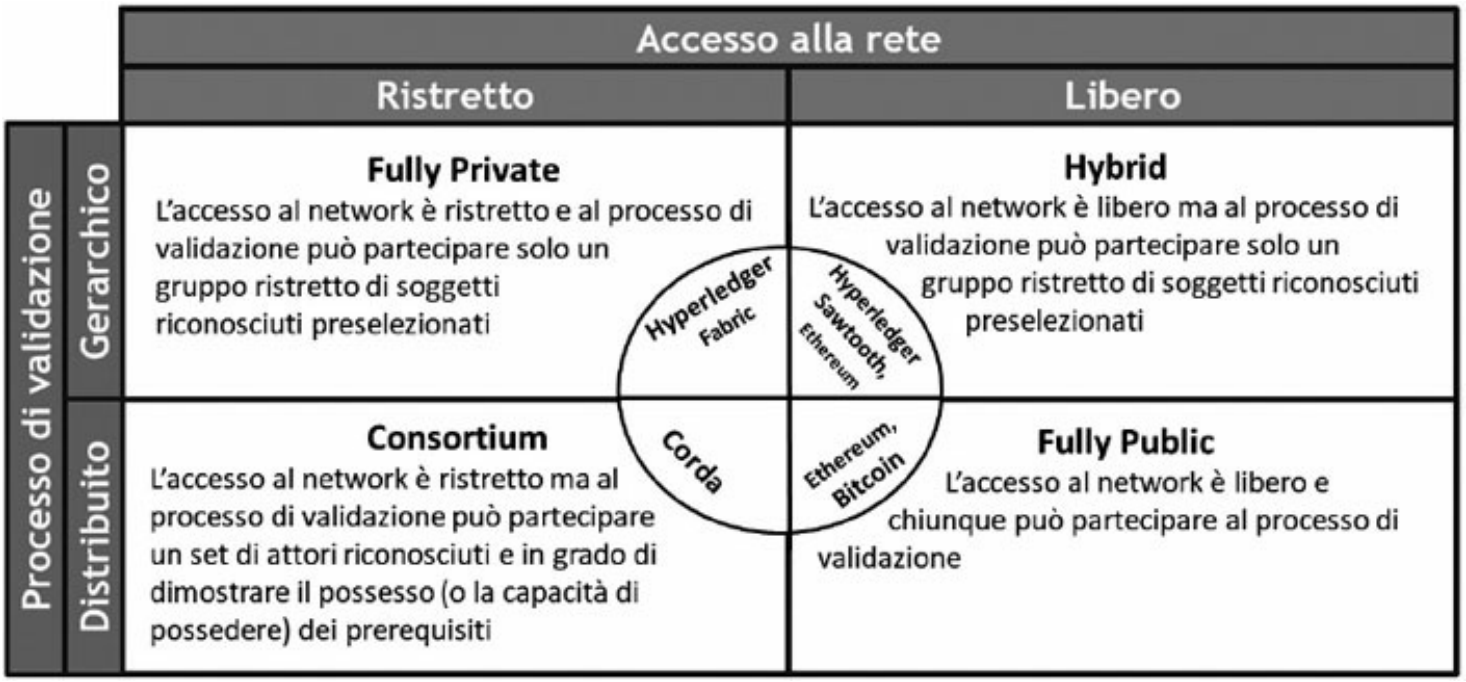

Figura 16.3 – Matrice delle blockchain.

17

Token e tokenizzazione

Riprendiamo ora un tema che abbiamo iniziato a trattare nella prima parte del libro, quando parlavamo del legame dell'asset nativo con il mondo degli scambi in un'economia reale.

L'asset nativo (e i sistemi che lo supportano) si rende molto utile in tutti

quei casi in cui si voglia ottenere garanzia dell'immutabilità di una transazione e della corretta esecuzione di un codice informatico che deve produrre un risultato inconfutabile. Può avere molto senso sfruttare una tecnologia che riesce a riprodurre il concetto di scarsità nel mondo digitale, per offrire prove incontrovertibili dell'avvenuta transazione di un bene fisico (pensiamo a una proprietà), ma anche di un bene immateriale (come la quota di un fondo, un diritto d'autore o un brevetto) se attribuissimo al criptoasset il valore di un gettone.

Ricordate quando esistevano ancora i gettoni con cui era possibile effettuare delle chiamate a pagamento tramite i

telefoni pubblici? Bene, il valore monetario attribuito al gettone era variabile nel tempo e il suo consumo (o utilizzo, se preferite) era legato a una logica programmata nel sistema telefonico associata allo "scatto"[84]. Facciamo ora un altro esempio. Avete presente gli autoscontri del luna park? Per salire sulla macchinina non è necessario avere alcun gettone, ma dovete possederne almeno uno e inserirlo nella gettoniera per poter avviare il vostro bolide e farvi un giro. Sebbene nessuno di noi vi abbia mai pensato, quel gettone conferisce un diritto la cui effettiva fruizione viene calcolata da un semplice meccanismo a

tempo e sul quale (diritto) ognuno di noi conviene fiducia in forza di un accordo tacito, implicitamente approvato nel momento in cui si va in cassa a comprare il gettone stesso.

In pratica, con l'inserimento del gettone nella macchinina, non avete l'immediata messa in moto del mezzo, ma avete la garanzia che, quando la corrente attivata centralmente dal cassiere presso cui avete cambiato la vostra valuta *fiat* (euro oggi, lire un tempo) per ottenere il gettone affluisce lungo il trolley, il vostro autoscontro parta.

Facciamo un ultimo esempio. Chi di voi non ricorda di aver usato, almeno una volta, le "palline" dei braccialetti (o

collanine) che all'interno di un villaggio turistico rappresentavano l'unico mezzo con cui poter acquistare una bibita o un accesso nella sauna, ovvero l'unico "sistema monetario" con cui era possibile negoziare all'interno del villaggio stesso? In questo caso la "pallina" assumeva un duplice significato: il primo era un'attestazione del diritto di appartenenza alla comunità (un diritto peraltro riscontrabile anche in correlazione con il periodo di vacanza scelto, poiché spesso le palline potevano cambiare dimensione o colore in funzione del mese o della settimana in cui la struttura le accettava); il secondo significato attribuito all'ammennicolo

era di rappresentare un'unità di conto, il cui valore-cambio era deciso dall'economia del villaggio (con due palline si poteva acquistare una bibita, con tre palline un accesso in sauna; ogni pallina verde valeva 1 euro, ogni pallina blu ne valeva 5 e così via).

Veniamo ora alle blockchain, certi che ognuno di voi abbia già compreso cosa volessimo introdurre: il gettone è un "token". Attribuendo un valore nominale al criptoasset o legando la legittimazione di un diritto al titolo che esso rappresenta, abbiamo creato quel legame tra un bene fisico e un asset nativo delle blockchain. Un asset che, in quanto digitale, è scambiabile su piattaforme Distributed Ledger e diviene

perno di un sistema transazionale, in cui la validità dei negozi giuridici sottostanti è garantita da un sistema matematico tale da ricreare quel rapporto di fiducia – anche – tra estranei, senza bisogno di una terza parte intermediaria.

Tipologie di token

Esistono diverse tipologie di token classificabili in funzione dell'uso tecnologico che di essi può essere fatto e del tipo di diritto nei medesimi incorporato. In relazione alla prima classificazione è importante sottolineare come l'impiego di Smart Contract che

vedremo nel successivo capitolo possa sostanziare la generazione di nuovi diritti, laddove siano eseguite, verificate e validate sulla blockchain eventuali clausole espresse all'interno dello stesso Smart Contract.

Ma procediamo con ordine e individuiamo le seguenti tre macrocategorie in cui è possibile far ricadere un token:

- *fiat* Pegged Token;
- Utility Token;
- asset Backed Token[85].

Fiat Pegged Token

I *fiat* Pegged Token sono una rappresentazione digitale di valute *fiat* che potremmo definire "aumentata". Con rappresentazione digitale di una moneta *fiat* intendiamo per esempio la Moneta Elettronica (o e-Money) ossia una moneta a corso legale smaterializzata digitalmente[86]. Cosa intendiamo invece con l'aggiunta del termine "aumentata"? Analogamente alla realtà aumentata (o augmented reality) un token di questo tipo è in grado di conferire alla moneta *fiat* delle caratteristiche speciali che possiamo riassumere come di seguito:

- **Programmabilità**.
  L'esecuzione di una transazione su blockchain può

essere vincolata a un set di regole predefinite e "cablate" all'interno del token che determinano come (o dove) può essere usata la *fiat* money rappresentata dal token stesso.

- **Frazionabilità delle fonti di liquidità**. La transazione in cui questo token è usato come mezzo di pagamento, consente di attingere da più fonti di liquidità e inviare il pagamento a diversi beneficiari, garantendo l'atomicità della transazione stessa.
- **Auditabilità**. Tutte le transazioni effettuate mediante

queste tipologie di token su una blockchain permettono di mantenere una traccia immutabile degli scambi avvenuti tramite la moneta *fiat* rappresentata su un registro distribuito verificabile da terze parti.

Analizzeremo alcuni casi di grandissima utilità di questi particolari token nella Parte IV di questo libro, quando parleremo di "moneta di scopo".

Prima di passare alle successive due categorie di token, chiariamo due aspetti importanti che riguardano i *fiat* Pegged Token:

1. Nel novero dei *fiat* Pegged

Token non è corretto includere ciò che, più comunemente, chiamiamo criptovalute (come per esempio i Bitcoin e tutte le sue derivazioni): queste ultime non hanno (né potrebbero avere, stante l'attuale regolamentazione) alcuna legittimazione di moneta *fiat* al di fuori dei propri network.

2. I *fiat* Pegged Token potrebbero essere utilizzati come mezzo di scambio anche al di fuori del network (per esempio in un'economia

reale, come valute complementari a quelle a corso forzoso), assolvendo sia le funzioni che abbiamo più volte descritto in precedenza con riferimento a ciò che abbiamo chiamato criptoasset sia gli obblighi derivanti da un set di regole definibili all'esterno del network (per esempio in un'economia di scopo o del territorio).

Utility Token

Appartengono a questa categoria quei

token che possono essere impiegati in un processo tecnologico, come per esempio l'uso di una applicazione software, lo sfruttamento di servizi di cloud, o più genericamente l'accesso e l'impiego di una qualsiasi piattaforma digitale in grado di prestare servizi di qualsiasi genere o di un genere specifico. Spesso il mercato di questi token è "agitato"[87] da un sovraffollamento di ICO (Initial Coin Offering), mediante le quali a fronte di una vendita di Utility Token corrisponde un preacquisto di servizi che verranno resi dalla futura piattaforma, ossia da ciò che dovrebbe rappresentare la realizzazione conclusiva del progetto digitale per cui

avviene il finanziamento tramite ICO. A differenza della precedente categoria di token, la possibilità che gli Utility Token acquistino una vendibilità tale da poter essere impiegati come mezzo di scambio in un'economia esterna al network è piuttosto risibile.

Cosa Significa ICO

ICO è l'acronimo di Initial Coin Offering. Le ICO sono una modalità, alla data in cui si scrive questo libro non ancora regolamentata, con cui una startup nel settore delle criptovalute

può raccogliere fondi.

I diritti incorporati negli Utility Token

Per la natura digitale dei token, quando si parla di Utility Token è molto spesso difficile distinguere i confini tra l'utilità meramente tecnologica e il diritto incorporato nei medesimi che può essere fatto rivalere contro terzi. Si pensi, per esempio, alla metafora degli autoscontri in un luna park. Una digitalizzazione del gettone di plastica acquistato alla cassa potrebbe assolvere contemporaneamente la funzione tecnica di accenditore della macchinina e la legittimazione a

effettuare almeno un giro sulla pista. In questo caso gli Utility Token possono essere assimilabili a titoli di legittimazione[88].

Asset Backed Token

In questa terza categoria sono ascrivibili quei token che rappresentano un diritto a essere convertiti in un altro bene, ovvero rappresentano una digitalizzazione non già di una valuta *fiat* (come nella prima categoria) bensì dell'asset sottostante, al quale conferisce liquidità e trasferibilità sulla blockchain[89]. In questo caso si tratta di token in grado di attribuire ai proprietari

alcuni diritti che possono essere esercitati nei confronti del soggetto che ha generato i token o eventualmente nei confronti di terzi. Sotto il profilo civilistico si potrebbe dire che questi token siano una sorta di titoli di credito, la cui disciplina è parzialmente contenuta nel codice civile (artt. 1992 ss. c.c.) e in parte in leggi speciali. La spendibilità di questi token su mercati esterni al network avrà un valore che, pur rimanendo ancorato al prezzo dell'asset sottostante, incorporerà il beneficio dipeso dalla digitalizzazione e dalla trasferibilità del criptoasset.

---

84. Il famoso "scatto telefonico" che ha

preceduto la tariffa a tempo, per capirsi.

85. Gli asset Backed Token possono chiamarsi anche con altri termini, fra cui ricordiamo: Security Token, Equity Token, Royalty Token.

86. Si veda anche l'Appendice A per una definizione completa di moneta elettronica.

87. Al momento in cui questo libro viene scritto si potrebbe dire "drogato".

88. Art. 2002 c.c.

89. Possono rappresentare per esempio quote societarie o certificati di credito.

PARTE IV
DISTRIBUTED COMPUTING

La democrazia divide gli uomini
in lavoratori e fannulloni.

Non è attrezzata per quelli
che non hanno tempo per lavorare.

Karl Kraus

18

Nel regno del Distributed Computing

Proseguendo nel nostro cammino di conoscenza delle blockchain, dopo aver compreso che cosa siano, come si formino e a che cosa servano, eleviamo il nostro sguardo verso un nuovo regno,

un dominio nel quale impera la ferrea logica del Distributed Computing. Addentriamoci dunque senza timore nell'analisi di ciò che una blockchain può rappresentare sotto il profilo di un efficientamento dei processi e in una maggiore relazione con la realtà delle cose e degli umani, non senza prima proporvi una semplice raffigurazione architetturale con cui siamo in grado, ora, di rappresentare l'evoluzione della blockchain (Figura 18.1).

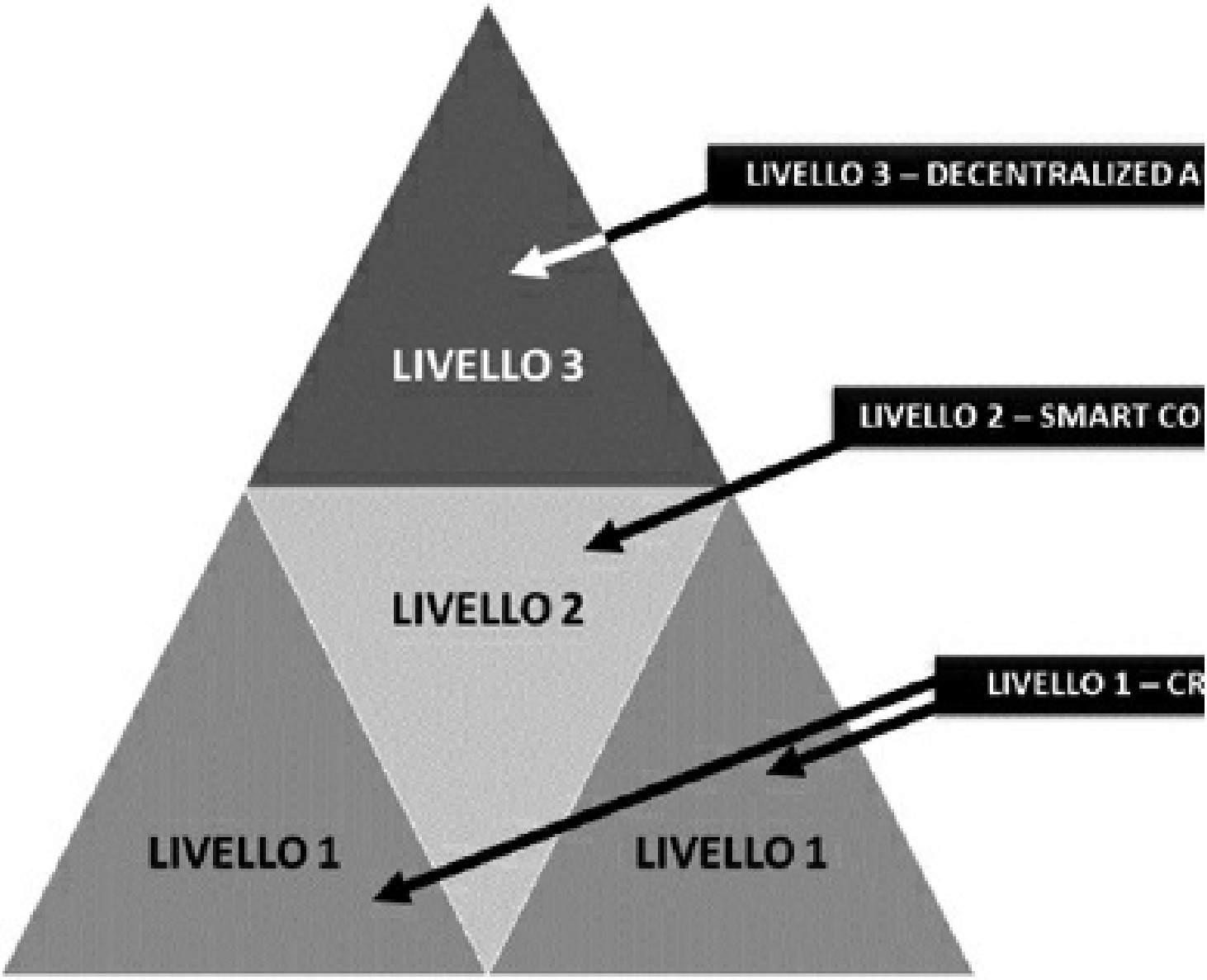

Figura 18.1 – L'evoluzione della blockchain.

I primi due livelli della piramide (1 e 2) sono stati oggetto di disamina rispettivamente nella Parte II e III di questo libro. In questa Parte IV

analizzeremo gli scenari, molti dei quali futuribili (ma non futuristici), che possono svilupparsi lungo il livello 3 della piramide.

Distributed Contract

Ricordate gli script trattati nella Parte II del libro, quando si è parlato di Blockchain dei Bitcoin? Lo script non è altro se non un microcodice informatico che accompagna ogni transazione sulla Blockchain e per il quale ciascun nodo è in grado di eseguire specifiche azioni, finalizzate a consentire (o impedire) di usare la disponibilità di criptoasset trasferita da un soggetto cedente a uno

cessionario. Le caratteristiche funzionali di questo microcodice eseguito da ogni nodo permettono di conferire l'aggettivo "programmabile" al flusso di token scambiati tra i diversi partecipanti. Con un'opportuna programmazione degli script mediante appositi linguaggi, è possibile determinare delle regole "incorporate" indissolubilmente nel token, che ne condizioneranno l'effettivo utilizzo.

Uno Smart Contract, altresì chiamato "Distributed Contract" (a sottolineare la logica applicativa distribuita con cui viene eseguito il microcodice), amplia la programmabilità ottenuta tramite l'uso degli script estendendosi ad appannaggio delle diverse tipologie di

token che abbiamo spiegato nel capitolo precedente, rendendo così condizionabile, in funzione di regole predeterminate, il negozio giuridico sottostante alla transazione in criptoasset.

Smart Contract

Smart Contract è la "traduzione" o "trasposizione" in codice informatico di un contratto, che permette di verificare in automatico l'avverarsi di determinate condizioni e di eseguire in automatico azioni (o dare disposizione

affinché si possano eseguire determinate azioni) nel momento in cui le condizioni determinate tra le parti siano raggiunte e appurate. Lo Smart Contract è basato su uno script che "legge" sia le clausole che sono state concordate sia le condizioni operative nelle quali devono verificarsi le condizioni stesse e si auto-esegue nel momento in cui i dati riferiti alle situazioni reali corrispondono ai dati riferiti alle condizioni e alle clausole concordate.

Se uno script è essenzialmente una lista di istruzioni allegata a ogni transazione che descrive come il successivo destinatario ricevente la criptovaluta dovrà o potrà gestire la transazione

stessa, tramite il suo uso si abilita l'esecuzione di Distributed Contract, consentendo un aumento del livello di automazione delle transazioni; si riesce così a limitare al massimo il coinvolgimento umano esterno, in tutti quei casi in cui è necessario. Tecnicamente parlando potremmo considerarli come dei contratti scritti in un linguaggio eseguibile da una macchina in grado di essere operati nel rispetto delle proprie clausole e senza intervento esterno[90]. Uno Smart Contract può ricevere informazioni in input, elaborarle sulla base delle regole definite ed eseguire delle azioni come output. Al pari dei propri simili cartacei

può prevedere obblighi, benefici e sanzioni per le parti contraenti. Poiché questi contratti eseguono automaticamente i termini dell'accordo, potrebbe rendersi particolarmente complessa l'applicazione di alcuni fra i principi tradizionali in materia contrattuale[91]. Dobbiamo pensare a uno Smart Contract come un codice informatico molto semplice che soddisfa – solamente – condizioni di tipo *if-then-else*. Per esempio, pagare un libro ordinato via Internet solo quando: il corriere lo ha consegnato, si sia verificato che corrisponda a quanto ordinato e che non sia danneggiato, siano scaduti i termini per l'esercizio

del diritto di recesso. Il codice può dimostrare in modo inconfutabile il verificarsi degli eventi di cui prima e l'auditabilità delle transazioni eseguite viene garantita dalla scrittura permanente sul Distributed Ledger.

Allo stesso modo, le parti potrebbero considerare l'opportunità di rinegoziare o modificare il contenuto dell'accordo. In questi termini, la versione originale del contratto rimarrà in rete mentre le modifiche contrattuali concordate *ex post* dalle parti saranno rappresentate in un *addendum*. Parimenti, le parti potrebbero inserire nel contratto una clausola arbitrale al fine di dirimere questioni attinenti alla responsabilità contrattuale.

Un aspetto molto importante che va tenuto in considerazione quando si scrivono degli Smart Contract incaricati di governare una serie complessa di transazioni e, soprattutto, dove l'entità degli scambi è direttamente proporzionale al valore reale del token, è la necessità di sottoporre a un assessment preventivo (tramite auditor esterni) l'intero ciclo di vita dei medesimi, prima di depositarli sulla blockchain.

Che cos'è una

DApp

DApp è l'acronimo di Decetralized Application, ossia un'applicazione decentrata sviluppata per creare ed erogare un servizio operato da Smart Contract su una blockchain. Le DApp possono avere un'interfaccia utente mediante cui è possibile fruire dei servizi.

Il ciclo di vita di una transazione governata da uno Smart

Contract

La Figura 18.1 mostra le fasi del ciclo di vita della transazione su blockchain governata da uno Smart Contract per il caso del libro ordinato via Internet del precedente esempio.

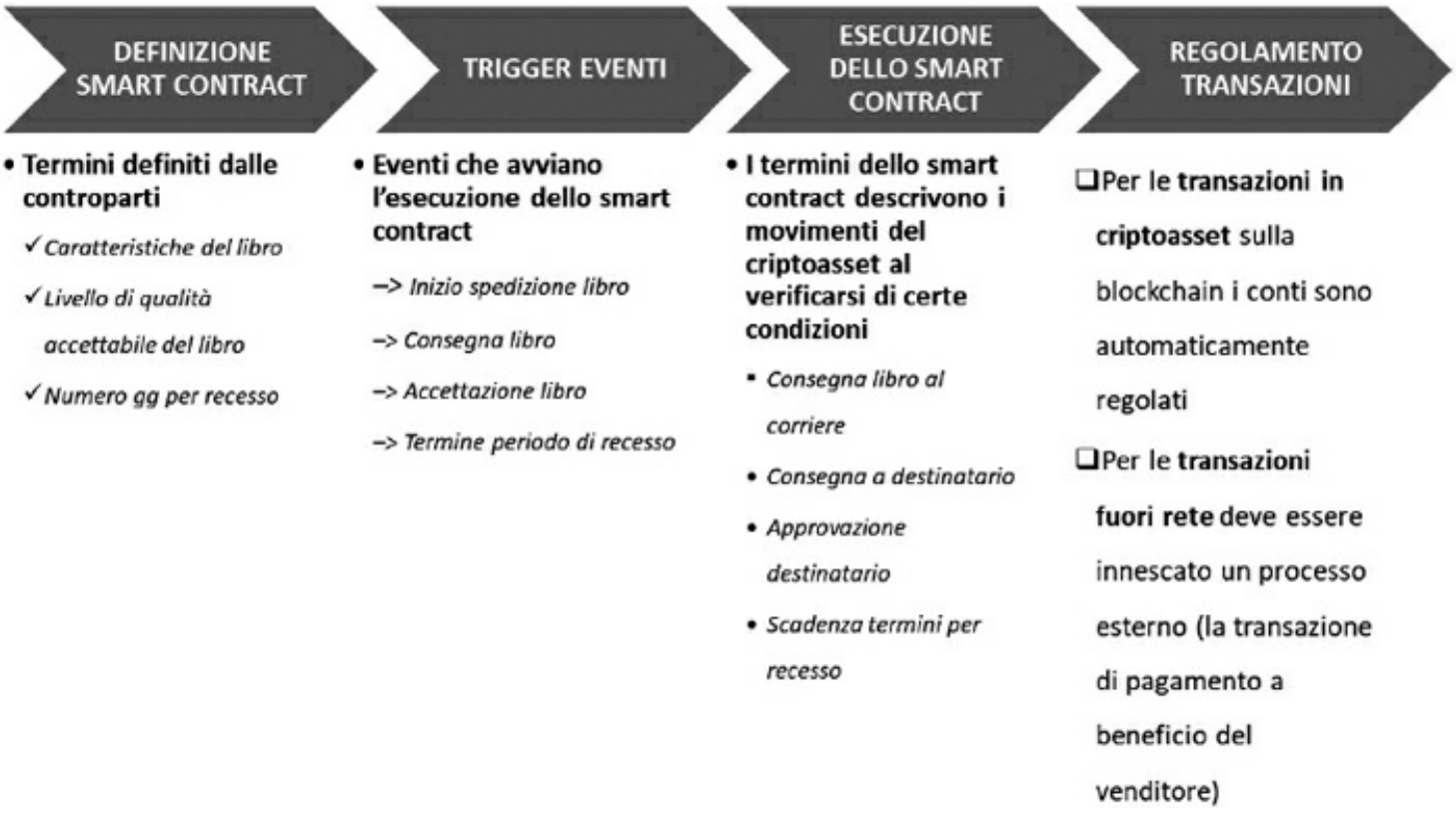

Figura 18.2 – Ciclo di vita di uno Smart

Contract.

Gli Smart Contract di Ethereum

Premesso che, come abbiamo illustrato nella Parte III di questo libro, dedicata alle DLT, sono diverse le blockchain che possono elaborare Smart Contract, Ethereum è senza dubbio una blockchain pubblica tra le più avanzate per quanto riguarda la scrittura del codice e l'elaborazione di Distributed Contract. Con essa, è possibile scrivere qualsiasi tipo di Smart Contract, ma solo se si è in possesso di una disponibilità di

criptoasset (l'Ether) sufficiente con cui pagare il potere di elaborazione[92].

In Ethereum gli Smart Contract sono microprogrammi cui è associato un piccolo database che è possibile modificare solo dal programma che lo controlla (codice e dati sono incapsulati). Il microcodice può ricevere dall'esterno messaggi che devono essere firmati digitalmente e che vengono esaminati dal medesimo per decidere in quale modo agire. L'esecuzione di uno Smart Contract avviene in una macchina virtuale presente su ogni nodo della rete chiamata EVM (Ethereum Virtual Machine): ogni step (ossia ogni

transazione) del contratto viene attivato da un messaggio per poi passare allo step successivo; questo avviene in modo automatico e indipendente in tutti i nodi della rete.

---

90. Il codice è di tipo open source, perciò chiunque può vedere come è implementato uno Smart Contract.

91. In via generale, i Distributed Contract propongono le stesse criticità in materia di privacy al pari di qualsiasi altra applicazione su Blockchain.

92. Per un maggiore dettaglio si veda quanto descritto nel Paragrafo “Ether e Gas: la moneta di scambio e il ‘carburante’ di Ethereum”.

DAO – Decentralized Autonomous Organization

Una DAO (Decentralized Autonomous Organization) è l'insieme di Smart Contract che rappresenta

un'organizzazione autonoma decentralizzata sulla blockchain e che ne automatizza il processo decisionale e la governance. Una DAO, come qualsiasi altra organizzazione del mondo reale, ha membri che hanno la capacità di raccogliere fondi e proporre diversi tipi di proposte e investimenti. Le proposte possono riguardare qualsiasi progetto che tragga un reale vantaggio dalla digitalizzazione dei processi attuata mediante il deposito e l'esecuzione di Distributed Contract sulla blockchain. Se approvate a maggioranza, queste proposte possono essere eseguite.

Le DAO, in breve

Sono organizzazioni imprenditoriali che operano come aziende digitali senza personalità giuridica e che agiscono attraverso regole codificate come programmi per computer (Smart Contract) eseguiti su una blockchain.

Come si può arrivare a una DAO

Possiamo immaginare un percorso evolutivo che conduce alla creazione di

una DAO seguendo questa logica. Partendo da un insieme di individui reali che condividono un'idea imprenditoriale, per la realizzazione della quale è necessario costruire una piattaforma digitale (per esempio per erogare servizi alla popolazione), la strada che può essere intrapresa per arrivare a costituire una DAO dovrebbe essere costellata da questi passaggi, qui intesi come acquisizione di consapevolezza e promessa d'impegno finalizzata alla creazione di un'organizzazione che governa la piattaforma:

1. **Partecipazione volontaria** estesa a chi è disposto a

investire nell'idea.

2. **Partecipazione collaborativa** rivolta a soggetti che decidono di lavorare insieme per il conseguimento comune dei risultati (realizzazione della piattaforma).

3. **Partecipazione cooperativa** rivolta a soggetti che sono disposti a investire nel progetto a fronte di un ritorno economico.

4. **Partecipazione distribuita** estesa tramite l'impiego della rete a soggetti che possono rendere disponibili risorse

computazionali (server, banda, spazio ecc.) e vogliono contribuire attivamente al funzionamento della piattaforma.

5. **Partecipazione decentralizzata** ulteriormente estesa con il fine di aumentare la scalabilità della piattaforma.

6. **Organizzazione autonoma decentralizzata**, che rappresenta il punto finale della proposta, ovvero l'avvio operativo dell'organizzazione che governa la piattaforma.

In una logica DAO, la piattaforma che sarà realizzata si basa su DLT e la governance dell'organizzazione verrà orchestrata tramite Smart Contract, la cui esecuzione viene garantita sulla blockchain. Questo significa che la DAO non ha un proprio management fisico che partecipa al governo dell'organizzazione ed è più corretto rappresentare l'esecuzione degli Smart Contract come un codice informatico eseguito da "agenti digitali" la cui impostazione è stata oculatamente scritta, questo sì, da persone fisiche. L'adesione alla DAO è offerta ai partecipanti che hanno creduto e investito nell'idea. Ogni partecipante può ricoprire ruoli diversi e ha accesso

alla piattaforma tramite:

a. l'impiego di un **Utility Token** per i soggetti passivi, ovvero gli utilizzatori della piattaforma;

b. l'impiego di un **asset Backed Token** per quei soggetti attivi che hanno investito nella piattaforma e che contribuiscono all'operatività in esercizio della stessa (per esempio i nodi);

c. l'eventuale uso di ***fiat* Pegged Token**, qualora i servizi resi dalla piattaforma dovessero integrare l'uso di monete *fiat*

(per esempio per pagare i fornitori);

d. l'uso di **criptovaluta** specifica della piattaforma per le transazioni di incasso e pagamento all'interno della piattaforma stessa e per la remunerazione dei nodi validatori.

Gli asset Backed Token possono (volendolo) essere tradable e potrebbero essere collocati mediante ICO (Initial Coin Offering)[93]. A parere di chi scrive, la possibilità oggi offerta di collocare gli asset Backed Token di una DAO mediante ICO in assenza di una regolamentazione di settore

rappresenta una debolezza che si riverbera in modo asincrono sulle opportunità insite in un progetto di Decentralized Autonomous Organization, mettendone a rischio l'intera sussistenza.

Le differenze fra DAO e DO

Per comprendere meglio il significato di organizzazione autonoma decentralizzata, laddove l'aggettivo "autonomo" è dirimente e assume una rilevanza che è propria di una DAO, è opportuno spiegare le differenze con una semplice Decentralized Organization.

Come ogni organizzazione tradizionale, un'organizzazione decentralizzata (DO) è governata da specifiche strutture divisionali e funzionali secondo cui le decisioni sono prese (a più livelli lungo la gerarchia aziendale) in base a un insieme predefinito di regole, controlli e codici di condotta. In una DO il processo organizzativo centralizzato viene decentralizzato. A tal fine, l'adozione di una blockchain segna il confine tra organizzazione gerarchica e struttura non territoriale, spontaneamente ordinata, un modello di organizzazione dove, sebbene il processo decisionale sia ancora controllato dagli esseri umani,

qualsiasi transazione interna ed esterna si verifica con un insieme incorruttibile di regole aziendali. Per esempio, le DO gestiscono direttamente sulla blockchain: sistemi di voto, contabilità, registro dei soci, produzione, scorte, ordini e così via. In queste organizzazioni decentralizzate le informazioni sono gestite ed elaborate da umani (non da macchine) che verificano il flusso delle informazioni. In questo modo gli umani continuano a esercitare una supervisione dell'organizzazione perché controllano, in qualche misura, le fonti delle informazioni, le regole e i codici di condotta aziendali.

Nel modello delle DAO,

differentemente da quello delle DO, il processo decisionale non è più controllato dagli umani, bensì è come se fosse nella responsabilità della DAO stessa, realizzato da un insieme di Smart Contract e di agenti autonomi tra loro interconnessi e tutti dotati di un capitale iniziale espresso in criptoasset. Attraverso un set di regole predefinito e auto-applicabile[94] codificato nei Distributed Contract, possono essere eseguite da un'organizzazione autonoma decentralizzata attività imprenditoriali o sociali (sia online sia offline) in completa autonomia, ovvero senza bisogno di alcun intervento umano.

Diversamente da ciò che talvolta

accade nelle tradizionali organizzazioni gerarchiche (o verticistiche), dove la gestione del flusso di informazioni e l'applicazione dei controlli può presentare opacità, le DAO provano a intervenire alla base del problema, creando un ambiente software open source basato su logiche di controllo partecipative tipiche delle blockchain (sia permissionless sia permissioned) in cui vigono protocolli di regolamento del consenso distribuito fra partecipanti (ossia di coloro che potremmo chiamare "Token Holders") trasparente, sicuro e verificabile.

I problemi ancora da

risolvere

Al momento in cui scriviamo questo libro, lo *status* legale delle DAO non è ancora del tutto chiaro. Le Decentralized Autonomous Organization sollevano diversi interrogativi in termini di responsabilità. Infatti, atteso che il loro "management" opera in modo automatico, sarebbe necessario stabilire di chi sia la responsabilità qualora una norma venisse violata: dello stesso sistema informatico? Di colui che ha creato il codice? O di chi utilizza il sistema? Inoltre, in quali rischi incorrerebbero i possessori degli asset Backed Token? Quali dovrebbero essere le coperture o le garanzie di questi

possessori? E a quale categoria potrebbero ascriversi (a quella dei "Token Holders")? Infine, ma non meno importante, quale regime fiscale dovrebbe rendersi applicabile alla DAO e ai "Token Holders"? Questi sono solo alcuni dei molti dubbi che riguardano le DAO e che devono essere quanto prima dipanati. Un buon punto di partenza potrebbe essere comprendere se le attuali norme giuridiche in materia societaria possano essere applicate anche alle DAO o se, viceversa, sia necessario creare nuova normativa atta a disciplinare queste nuove entità. Insomma, in parole povere, urge una regolamentazione.

Cosa è successo con "The DAO"?

"The DAO" (volutamente incluso fra doppi apici) ha rappresentato un evento critico molto importante – per alcuni aspetti ha costituito un precedente – nell'evoluzione di Ethereum. Ne avevamo accennato in precedenza al Capitolo 15, poiché ha dato origine alla Hard Fork di Ethereum ed è importante per capire le logiche evolutive di una qualsiasi DAO.

Nata nel 2016, "The DAO" era a tutti gli effetti una Decentralized Autonomous Organization "stateless" (ossia non creata in uno specifico stato

del nostro pianeta, in quanto virtuale). Costruita su Ethereum, intendeva raccogliere capitali (tramite lo scambio di DAO token a fronte di Ether, la criptovaluta di Ethereum) da investire su progetti previamente valutati da un comitato e poi posti in votazione ai possessori di DAO token. Questi "Token Holders" (continuiamo a chiamarli così, per comprenderci) potevano esprimere il proprio voto, proporzionale alla quantità di DAO token nella loro disponibilità, per determinare su quali progetti sarebbero poi stati convogliati i capitali. "The DAO" è stata realizzata con una serie di passaggi tipici di una ICO: sito Internet per fornire informazioni, diffusione di un

whitepaper in cui viene descritto il progetto, audit del codice sorgente degli Smart Contract utilizzati, accordi con alcuni exchange provider (i cosiddetti "cambiavalute virtuali") per permettere lo scambio dei token una volta acquisiti e così via.

Nel giro di pochi mesi gli organizzatori di "The DAO" riuscirono a raccogliere circa 150 milioni di dollari, ma a causa di un attacco perpetrato a opera di chi aveva individuato alcune vulnerabilità nel codice della piattaforma, il 18 giugno 2016 in poche ore andarono in fumo circa 70 milioni di dollari. La vicenda diede luogo a una serie di discussioni e

confronti e portò alla scissione della blockchain Ethereum che vi abbiamo raccontato nel paragrafo "La profonda frattura venutasi a creare sul concetto di base di una blockchain" (Capitolo 15), nonché condusse la SEC (Securities and Exchange Commission, ossia l'ente federale statunitense preposto alla vigilanza della borsa valori, concettualmente simile alla nostra Consob) ad analizzare la vicenda per comprenderne la possibile riconducibilità nel novero dell'attività di collocamento di strumenti finanziari e, di conseguenza, per vagliare se nel caso di specie fosse stata applicabile la Securities Law[95].

La vicenda ha messo in luce, in tutta la propria avventatezza, sia uno spaccato giuridicamente rilevante, dipeso dall'assenza di una normativa di settore, sia una vulnerabilità della piattaforma per annullare le conseguenze della quale, oltre a essersi originata la scissione che abbiamo ricordato in precedenza sulla blockchain di Ethereum, si sono posti in essere dei sistemi che compromettono, nel senso più profondo, l'assunto di base su cui si è sviluppata Ethereum (e, più in generale, tutte le blockchain pubbliche e permissionless): l'immutabilità della storia delle transazioni.

---

93. Si veda anche il paragrafo "Utility Token" del Capitolo 16.

94. Si parla in questo caso di un enforcement automatico, ossia scritto nel codice.

95. L'indagine condusse la SEC a considerare i DAO token alla stregua di strumenti finanziari, con conseguente applicazione della Securities Law dalla quale deriva l'obbligo per l'ente emittente di registrare le offerte e vendite degli strumenti e, correlativamente, con il conseguente obbligo di registrazione per i soggetti che offrivano piattaforme di scambio (trading) dei token suddetti quali National Securities Exchange (per un approfondimento si veda il report della SEC del 25 luglio 2017 reperibile sul sito dell'autorità: https://www.sec.gov).

PARTE V
GLI AMBITI APPLICATIVI CROSS-INDUSTRY

Il prezzo è quello che paghi.
Il valore è quello che ottieni.

Warren Buffett

20

Oltre alle criptovalute c'è di più

Riprendendo la Figura 18.1, nella quale abbiamo rappresentato l'evoluzione su tre livelli della blockchain, ove ci soffermassimo solo sul livello 1 potremmo riconoscere che la blockchain

a supporto delle criptovalute garantisce l'unicità delle transazioni e l'immutabilità delle stesse, impedendo, nel contempo, che siano validate transazioni fittizie che potrebbero aggiungersi alla catena di blocchi e vanificando, parimenti, la possibilità di modificare ciò che è avvenuto in precedenza. Salendo di livello abbiamo altresì compreso anche che gli algoritmi su cui si basa la blockchain consentono l'impiego di tecniche di scripting con cui è possibile abilitare l'esecuzione di Smart Contract. Uno Smart Contract è, dunque, un metodo di utilizzo delle criptovalute per formare accordi attraverso la blockchain, sfruttando opportunamente il quale è possibile

raggiungere altri scopi che vanno ben oltre il concetto di valuta virtuale. Un esempio di applicazione degli Smart Contract a livello 2 della piramide di Figura 18.1 sono i cosiddetti "Colored Coins", ossia dei dati aggiuntivi (attributi) pubblicati e gestiti sul Distributed Ledger che trasformano i "coins" in "token" al fine di poter essere impiegati per rappresentare qualsiasi cosa (anche non una valuta). Nel Capitolo 17 abbiamo dettagliatamente spiegato quali siano le tipologie di token e il loro impiego funzionale alla blockchain.

Andiamo ancora oltre. Se associassimo alla blockchain il

significato di Internet of Value presentato all'inizio della Parte II di questo libro, vedremmo una rete digitale di nodi che si trasferiscono valore, anche in assenza di fiducia, attraverso un sistema di algoritmi e regole criptografiche tale da consentire il raggiungimento di un unico consenso sulle modifiche di un registro distribuito che tiene traccia dei trasferimenti di valore, tramite asset digitali univoci. In questo modo non è difficile prevedere un impiego di questa tecnologia in campi anche molto diversi da quello delle criptovalute.

Se si ipotizza di scambiare su blockchain "bitcoin" come "token" e non come "valuta", ecco ottenersi una sorta

di registro contabile potenzialmente inviolabile, che tiene traccia di tutte le transazioni eseguite. Una Distributed Ledger Technology così intesa permetterebbe il trasferimento di proprietà di "gettoni digitali" a cui possono essere associati svariati beni e diritti nel mondo esterno (asset).

In questa Parte IV del libro ci dedicheremo alla presentazione di alcuni ambiti applicativi cross-industry per cui riteniamo possa rendersi utile studiare l'applicazione della blockchain; tutti i contesti che vedremo non sono riferiti alle criptovalute, per quanto molti di loro siano implementabili sul livello 1 della piramide di Figura 18.1

proprio “grazie” alla presenza di un criptoasset.

Un primo assaggio? Assumiamo, per esempio, di poter considerare come asset la prova dell’identità digitale di un individuo. A ciascun soggetto identificato[96] è possibile attribuire un token[97] che lo autorizza a compiere azioni “fisiche” (ossia nel mondo fisico) sfruttando una tecnologia digitale distribuita e l’esecuzione di specifici Smart Contract.

La parte che segue è tratta da “Criptovaluta, validatori e tutti i vantaggi dell’identità digitale”[98]:

> A titolo prettamente

esemplificativo, riporterò due possibili casi d'uso della blockchain così come presentata, volutamente (e provocatoriamente) tra loro molto distanti, ma accumunati dal medesimo impiego di una Distributed Ledger Technology: **sostegno ai processi di KYC** (Know Your Customer), **supporto alla sharing economy**. Nel primo caso, la blockchain potrebbe essere impiegata (per esempio da banche) nelle fasi di identificazione e verifica del cliente,

agendo come database di identità digitali blindate e crittografate, cui è possibile accedere in alternativa a database centralizzati. Ipotizzando uno scenario di "Permission Ledger" (accessibile solo da un gruppo di istituti finanziari, per esempio), si potrebbe migliorare l'efficienza dell'intero processo: digitalizzazione delle fasi di rilascio e verifica delle identità digitali, automazione di alcuni passaggi intermedi

mediante l'adozione di specifici Smart Contract, che controllano (e garantiscono) la corretta esecuzione delle regole. Nel secondo caso, l'industria che si basa sulla sharing economy può trarre innumerevoli vantaggi dall'adozione di una Distributed Ledger Technology, mediante cui sono gestite le identità digitali. Se s'immagina di integrare una simile tecnologia direttamente all'interno dei motori di ricerca che iniziano un

rapporto fra persone che non si conoscono, per poi arrivare a stabilire un accordo contrattuale fra di essi (l'uso di un locale in affitto, piuttosto che un passaggio in auto), è facile intuire come la blockchain possa contribuire alla finalità di garantire identità e reputazione di chi sta partecipando alla transazione. Anche in questo caso, l'intero processo potrebbe chiudersi in modo totalmente automatizzato,

mediante l'esecuzione di uno specifico Smart Contract che sovrintende – anche – l'incasso contro prestazione, qui inteso come trasferimento di fondi (*fiat* money) dal fruitore del servizio al beneficiario.

---

96. L'identificazione e il rilascio delle credenziali può avvenire a opera degli IdP (Identity Provider) come spiegato nel paragrafo "Un impiego virtuoso della Blockchain" (Capitolo 12).

97. Potremmo chiamarlo "Utility Token" con diritti incorporati, come abbiamo descritto nel Capitolo 17.

98. Garavaglia R., “Criptovaluta, validatori e tutti i vantaggi dell’identità digitale”, *Cor.Com*, Anno XII, n.12, settembre 2016.

La blockchain in contesti cross-industry

Caratteristiche e benefici

Prima di introdurci nei diversi ambiti

cross-industry nei quali l'adozione della blockchain potrebbe recare beneficio, riassumiamo le caratteristiche basilari di una piattaforma DLT che usa i protocolli della blockchain descritti nelle Parti II, III e IV di questo libro, percorrendo i tre livelli della piramide riportata nella Figura 18.1.

A livello 1, la gestione dei criptoasset per cui sono nate blockchain come quelle per i Bitcoin (e per tutte le sue biforcazioni) e la presenza di un incentivo per la validazione delle transazioni propongono le caratteristiche di base illustrate nella Figura 21.1.

Sulla base delle peculiarità evidenziate possiamo riassumere i benefici nell'adozione di una DLT

basata sui protocolli della blockchain, in particolare quelli che emergono dal solo livello 1, come di seguito:

1. **Sicurezza ottenuta tramite l'impiego di tecniche criptografiche avanzate**. La crittografia alla base delle blockchain è un metodo molto efficace per verificare l'identità digitale, che permette di aumentare la sicurezza e la protezione dei dati in qualsiasi sistema che ne richieda un impiego affidabile.
2. **Immutabilità e irreversibilità**. L'uso di una

DLT basata sui protocolli della blockchain permette di sviluppare piattaforme di rete sicure dove la trasparenza si rende apprezzabile e nelle quali è possibile consentire un accesso, parimenti trasparente e tracciabile, da parte delle autorità che regolano le norme di settore.

3. **Assenza di una terza parte "trusted"**. Grazie all'implementazione di diversi protocolli di consenso distribuito, è possibile avviare transazioni tra soggetti che non devono

necessariamente conoscersi e tra i quali non è richiesto un rapporto di fiducia *ex ante*, anche in assenza di intermediari terzi.

Figura 21.1 – Le caratteristiche basilari di una piattaforma DLT che impiega la blockchain a

livello 1.

Al livello 2 della piramide, la capacità offerta dagli Smart Contract di eseguire in automatico azioni controllate e validate grazie al supporto del livello 1, di reagire a input anche esterni al network e di produrre output che possono avviare azioni altrettanto esterne alla blockchain, è correlata a una serie di caratteristiche basilari che riportiamo in Figura 21.2.

Anche in questo caso, sulla base delle peculiarità evidenziate, possiamo riassumere i benefici nell'adozione di una DLT basata sulle feature di livello 2 come qui di seguito:

1. **Programmabilità della moneta** grazie alla presenza nelle transazioni di regole scritte che vengono eseguite in modo sincrono con la transazione stessa, tramite script e Smart Contract.
2. **Impiego di Smart Contract** tale da consentire un efficientamento per tutti quei processi che per loro natura richiedono momenti approvativi intermedi consecutivi, nella esecuzione dei quali è fondamentale avere livelli di garanzia elevati e dove la possibilità

di integrazione con il mondo esterno delle cose e degli oggetti (IoT e IoeT[99]) si rende necessaria senza il bisogno di un intervento umano.

3. **Interazione con il mondo esterno** grazie alla gestione di sensori programmati dagli Smart Contract e l'integrazione con gli oracoli[100].

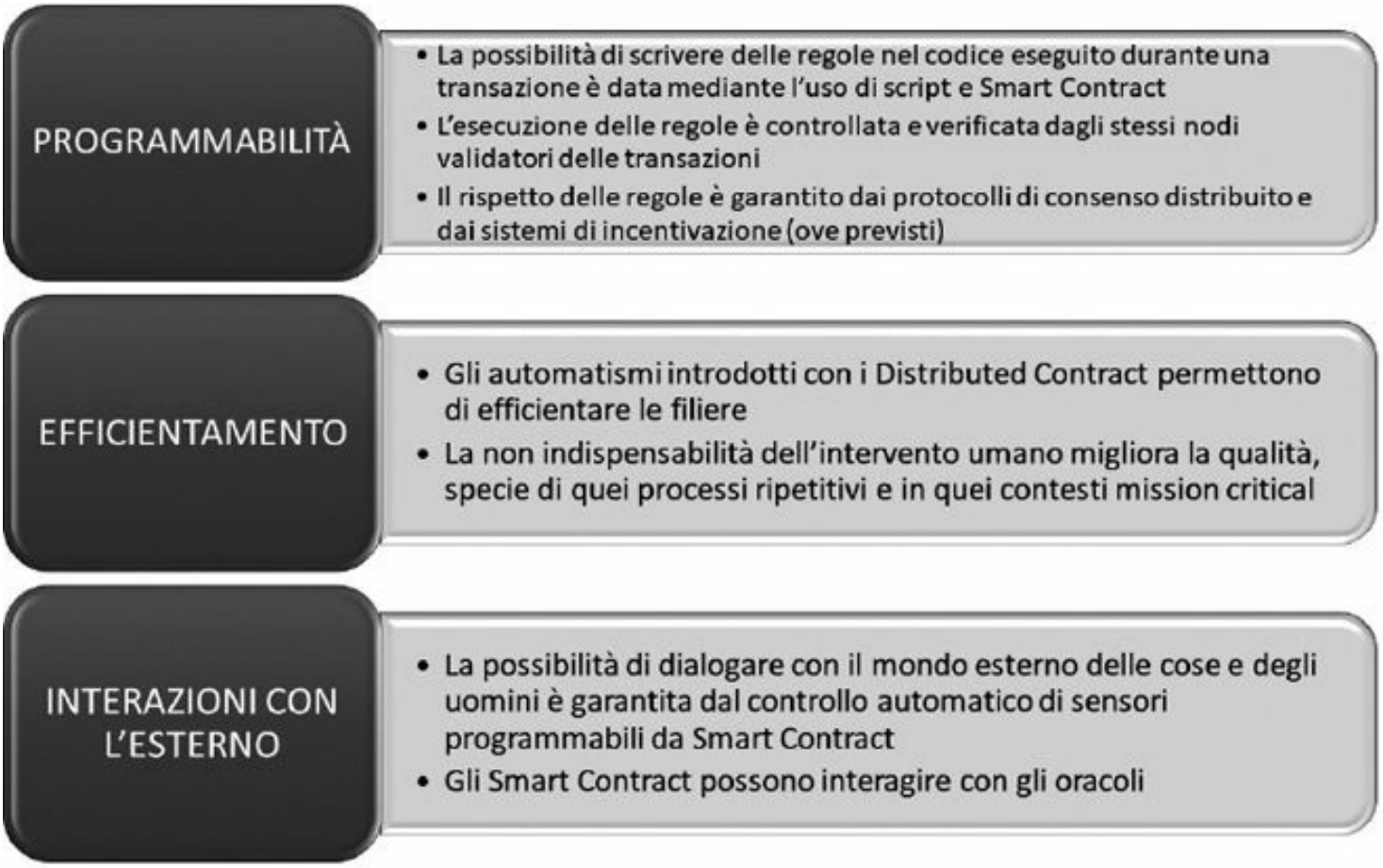

Figura 21.2 – Le caratteristiche basilari di una piattaforma DLT che impiega la blockchain a livello 2.

Salendo ulteriormente di livello nella piramide della Figura 18.1, l'opportunità offerta dalle DApp di eseguire applicazioni anche complesse e

la possibilità di organizzarne la gestione in una DAO presenta una serie di caratteristiche basilari che riportiamo in Figura 21.3.

Figura 21.3 – Le caratteristiche basilari di una piattaforma DLT che impiega la blockchain a livello 3.

Anche in questa circostanza, sulla base delle particolarità evidenziate, possiamo sintetizzare i benefici nell'adozione di una DLT basata sui servizi di livello 3 come di seguito:

1. **Esecuzione di interi processi** in modo automatico e autonomo con l'affidabilità garantita dalle implementazioni di livello 1 e 2 della blockchain.

2. **Governance decentralizzata e distribuita**, la cui affidabilità è garantita da un insieme correlato di macchine e di umani che interagiscono

autonomamente fra loro nel rispetto di regole comuni, secondo un algoritmo open source, in trasparenza e nella consapevolezza di essere parte attiva e integrante del sistema.

3. **Efficientamento delle procedure burocratiche** tramite il riuso di framework programmati e riduzione del time-to-market per nuove iniziative ad alto contenuto tecnologico.

I principali driver che

identificano i migliori casi d'uso

Posto che non sarebbe intellettualmente corretto asserire (o anche solo pensare) che le blockchain siano la panacea di ogni male, è altrettanto opportuno individuare un insieme minimale di requisiti che, se soddisfatti (anche solo parzialmente), dovrebbero suggerire il giusto percorso per un'analisi dei KPI e dei CSF. Per valutare in prospettiva i casi d'uso delle blockchain più appropriati, si possono utilizzare diversi fattori chiave di valore, fra cui si annoverano:

- **Semplificazione operativa**

- Riduzione intervento manuale nei processi che possono essere automatizzati
- Riduzione del rischio di errore

- **Ottimizzazione organizzativa**
  - Snellimento delle procedure burocratiche
  - Efficientamento gestione dispute e controversie
  - Supporto alle misure anticorruzione
  - Attivazione dei benefici

di una democrazia partecipativa

- Ridistribuzione del valore alla comunità

- **Minimizzazione frodi e contraffazione**
  - à Miglioramento ed efficientamento della tracciabilità di filiera
  - Marcature temporali “indelebili” e a prova di corruzione
  - Ottimizzazione dei controlli da parte delle autorità di settore incaricate di vigilare sui

processi

- → Miglioramento della trasparenza

- **Riduzione dei rischi di controparte**
  - → Diminuzione della necessità di affidamento alle controparti per l'adempimento agli obblighi, poiché gli accordi possono essere codificati mediante la creazione di Smart Contract ed eseguiti in un ambiente condiviso, partecipativo e tecnicamente immutabile

- **Ottimizzazione dei processi di compensazione e regolamento**
  - → Disintermediazione delle terze parti che supportano la verifica e la convalida delle transazioni finanziarie
  - → Diminuzione dei rischi tecnici
  - → Diminuzione dei rischi di reputazione
  - → Possibile impatto positivo sui rischi di sistema (specie se in combinazione con

l'attenuazione dei rischi di controparte, di cui all'elenco precedente)

Anche sulla base di queste valutazioni, nel prosieguo proporremo una sintesi delle possibili applicazioni basate su DLT e blockchain raggruppate per le seguenti aree di applicazione:

1. Agrifood
2. Assicurazioni
3. Banking
4. Digital marketing
5. Donazioni
6. Finance
7. Identità digitale

8. Media industry
9. Settore pubblico
10. Sharing economy
11. Trasporti
12. Turismo
13. Utilities
14. Welfare

Ogni area sarà analizzata tramite la raffigurazione in quadranti sulla matrice in Figura 21.4 dove:

- al centro è riportato il settore di riferimento analizzato, alla luce dei potenziali benefici conferibili da progettualità basate su DLT;

- nel quadrante **BLOCKCHAIN LIV. 1** sono riportati i casi d'uso che più beneficerebbero dall'applicazione di una DLT che presenta le caratteristiche individuate nella Figura 21.1;
- nel quadrante **BLOCKCHAIN LIV. 2** sono riportati i casi d'uso che più beneficerebbero dall'applicazione di una DLT che presenta le caratteristiche individuate nella Figura 21.2;
- nel quadrante **BLOCKCHAIN LIV. 3** sono riportati i casi d'uso che più beneficerebbero dall'applicazione di una DLT che presenta le caratteristiche

individuate nella Figura 21.3;

- nel quadrante **INDIFFERENZA BLOCKCHAIN** sono riportati i casi d'uso per cui l'applicazione di una DLT sarebbe indifferente sul piano dei potenziali benefici.

I cerchi all'interno dei quali sono numerati i casi d'uso si caratterizzano per la dimensione dell'area, che rappresenta in proporzione l'apporto quantitativo di benefici al caso d'uso in esame legati all'adozione di una DLT specifica.

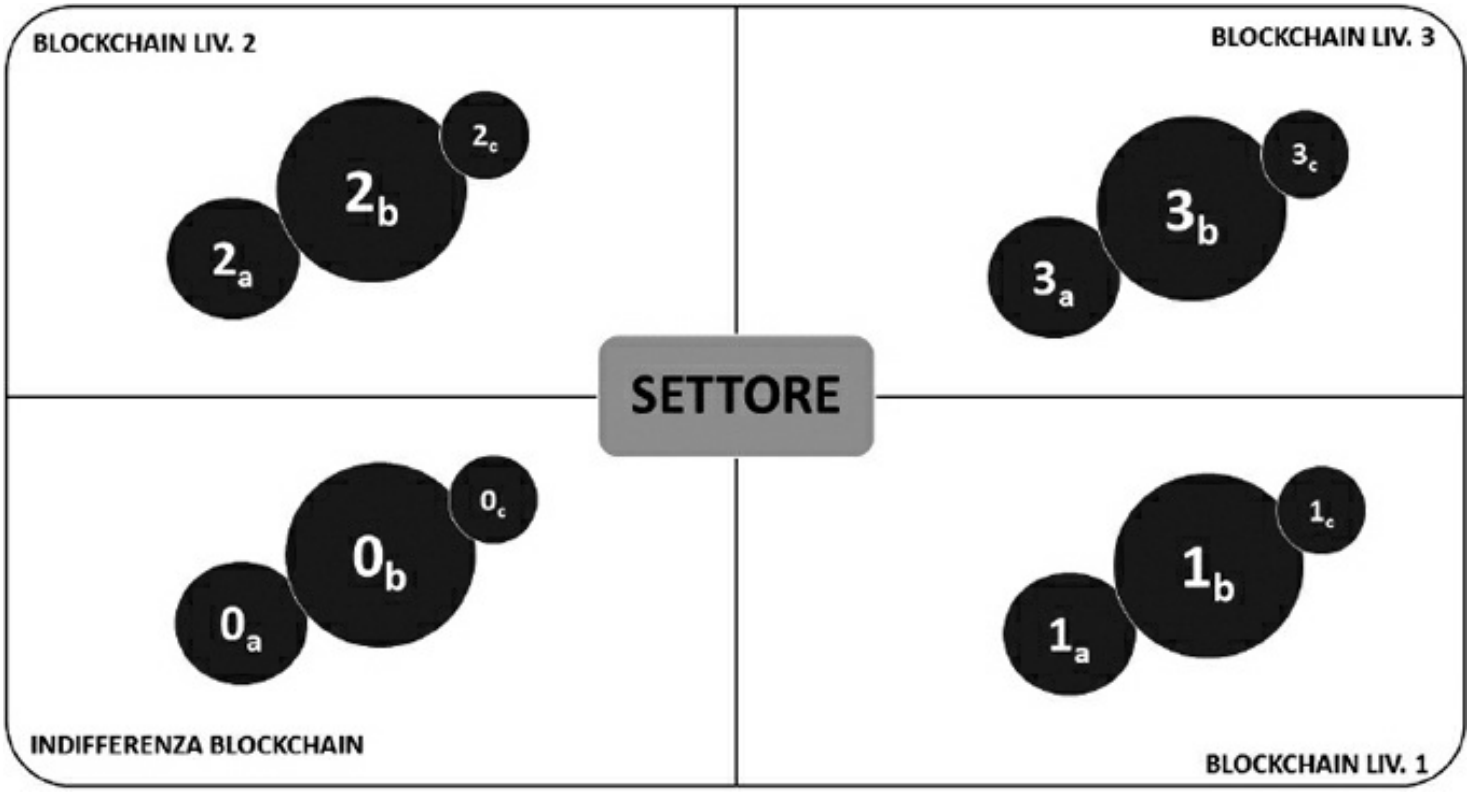

Figura 21.4 – Matrice settori/benefici da DLT.

---

99. Con "IoT" e "IoeT" si intende rispettivamente Internet of Things e Internet of everyThings; si veda anche la Parte VI del libro, "Scenari e strategie", per un approfondimento delle opportunità offerte in questo specifico ambito, ritenuto fra i più rilevanti sotto il profilo strategico in una profondità temporale

di medio-lungo termine.

100. Gli oracoli fanno da ponte tra il mondo reale e la blockchain; in sostanza sono dei software che verificano il rispetto delle condizioni degli Smart Contract.

Settori di applicazione

Riportiamo, rigorosamente in ordine alfabetico, i settori di applicazione per le DLT che abbiamo esaminato.

Agrifood

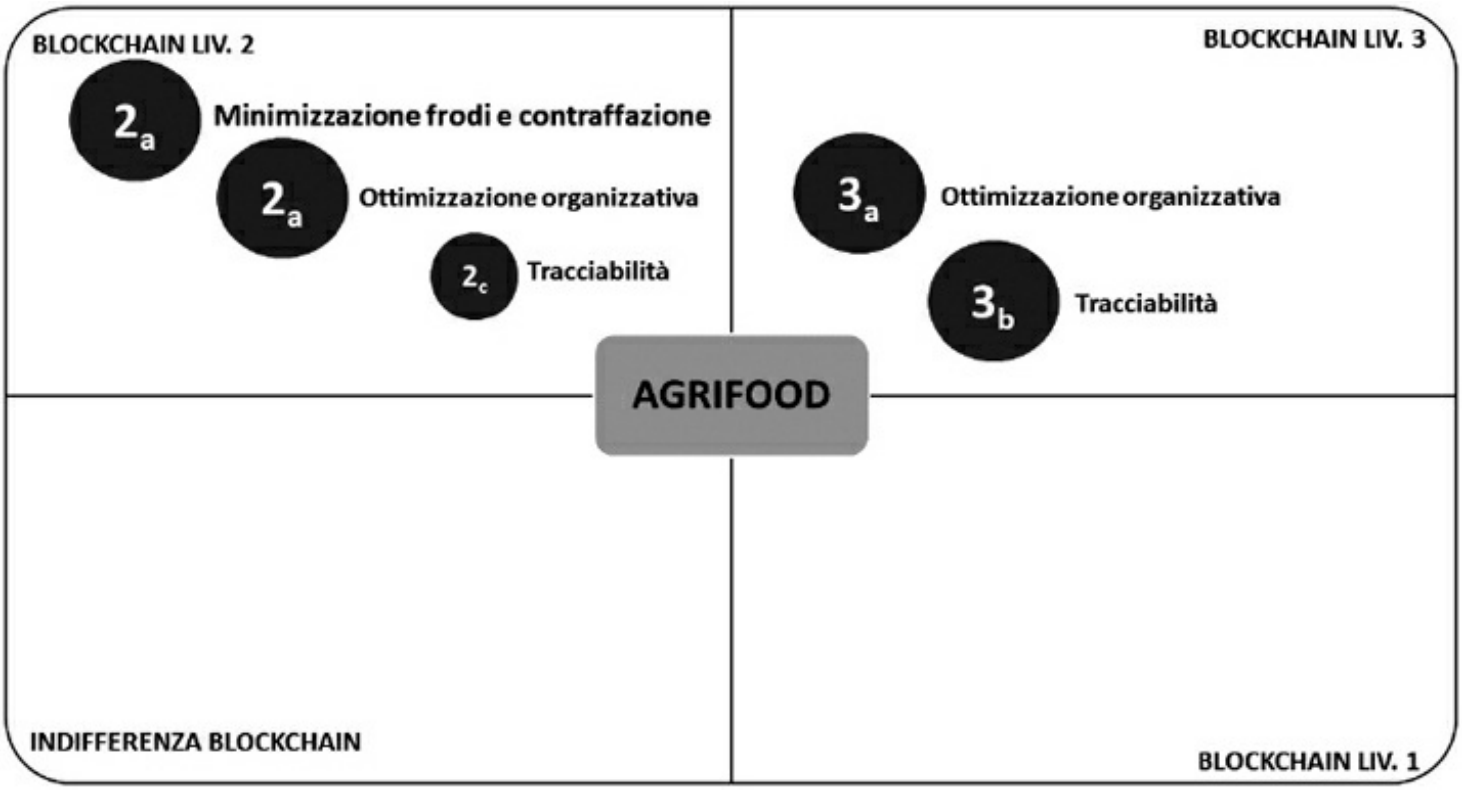

Figura 22.1 – Benefici DLT per Agrifood.

Assicurazioni

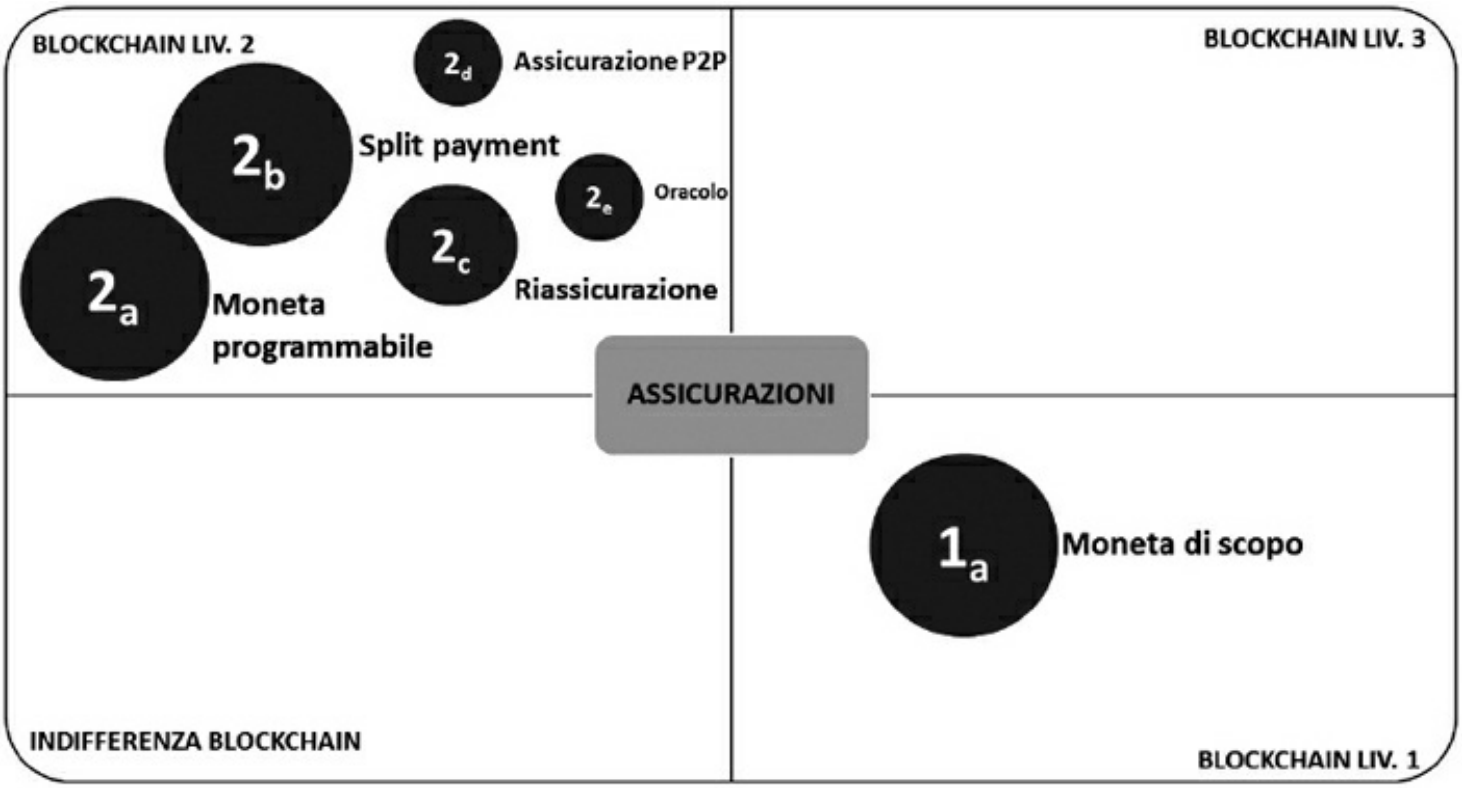

Figura 22.2 – Benefici DLT per Assicurazioni.

Banking

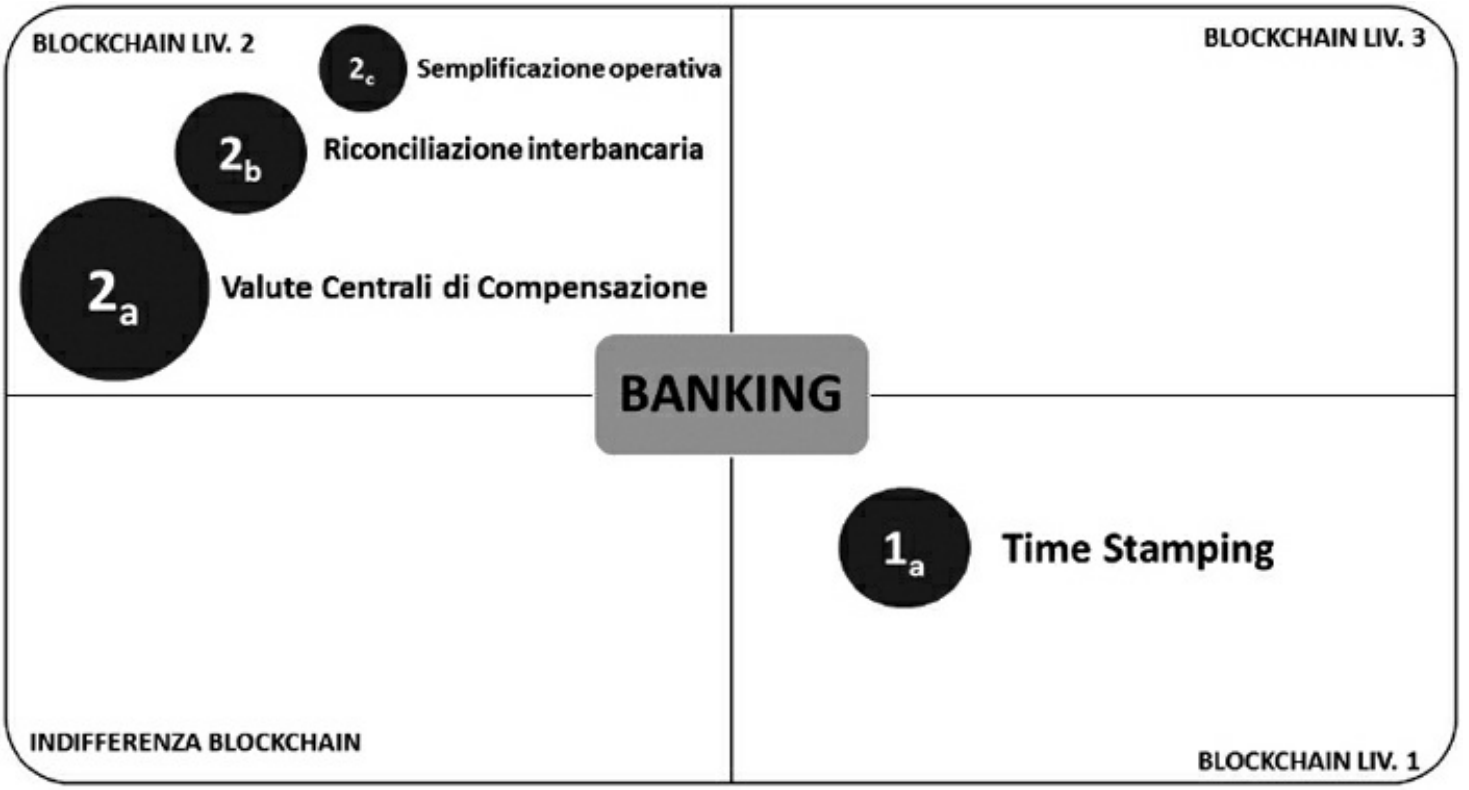

Figura 22.3 – Benefici DLT per Banking.

Digital marketing

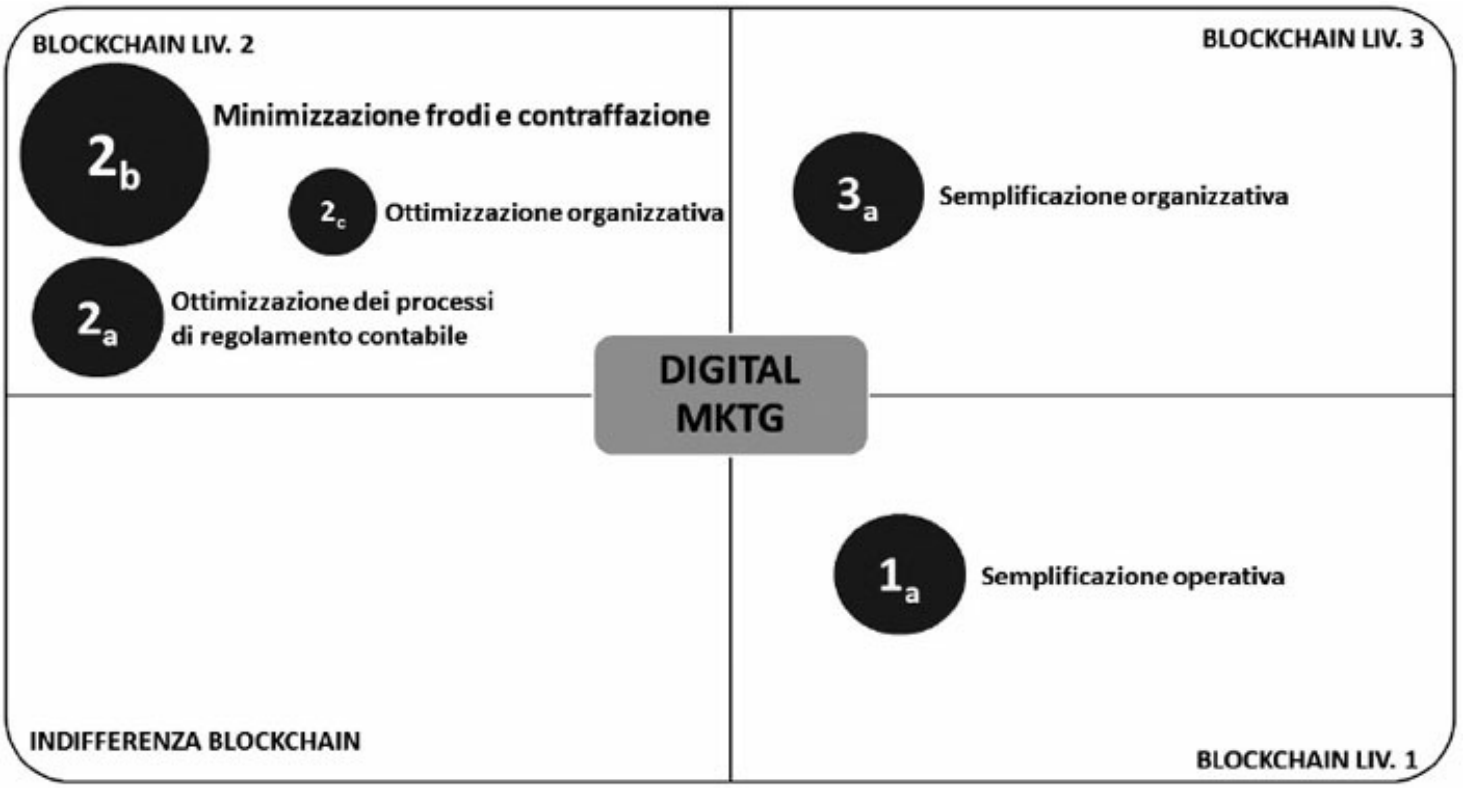

Figura 22.4 – Benefici DLT per Digital marketing.

Donazioni

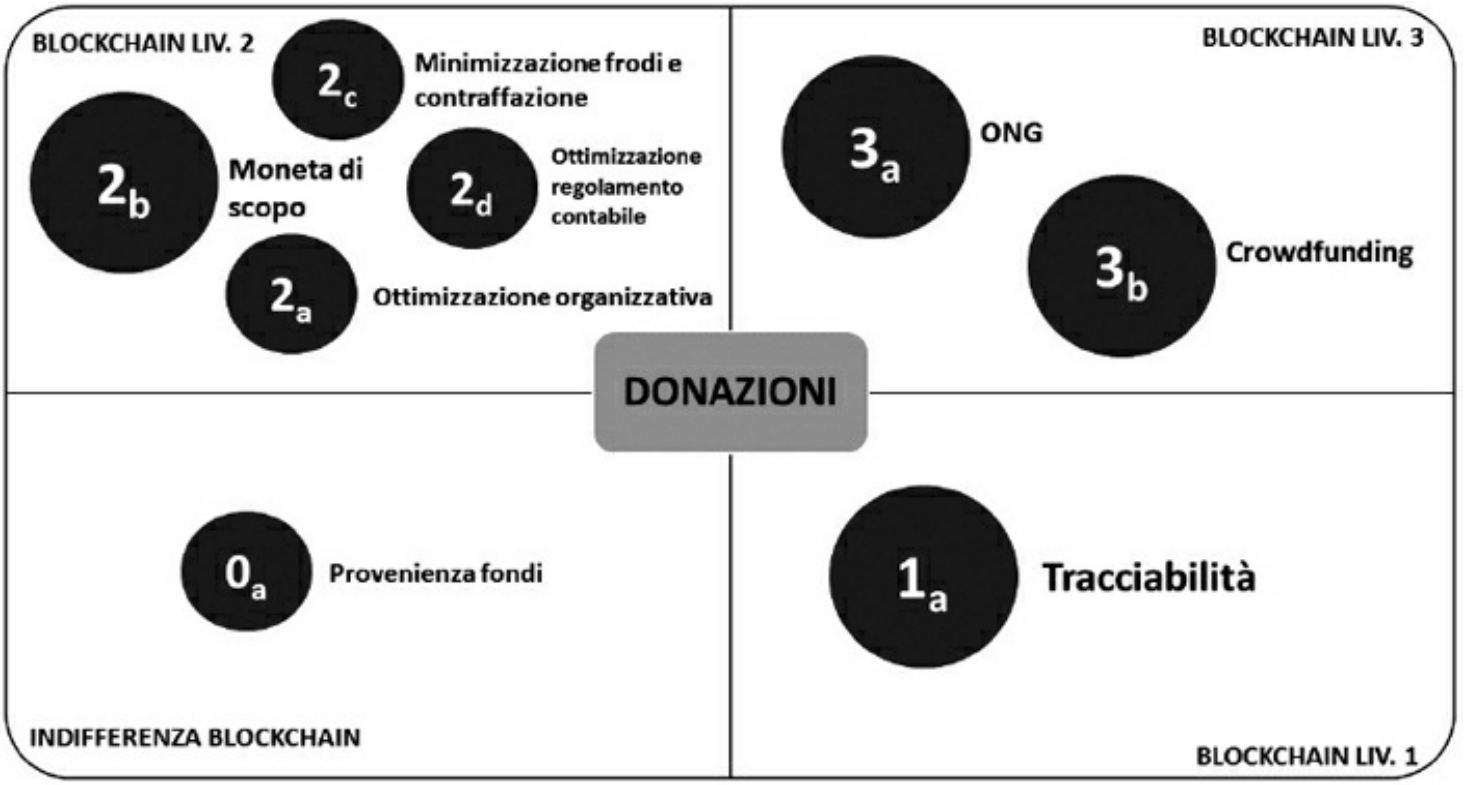

Figura 22.5 – Benefici DLT per Donazioni.

Finance

Figura 22.6 – Benefici DLT per Finance.

Identità digitale

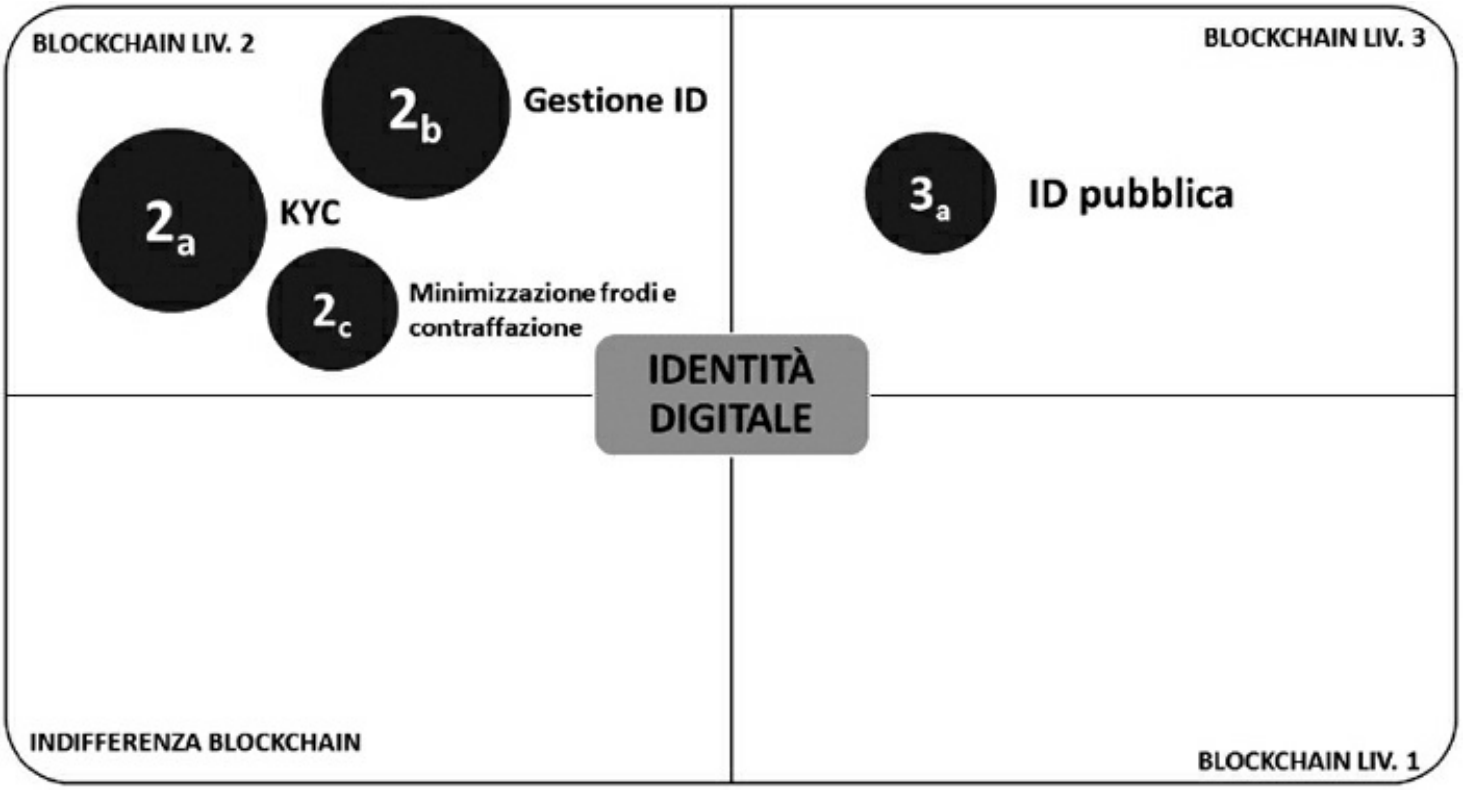

Figura 22.7 – Benefici DLT per Identità digitale.

Media industry

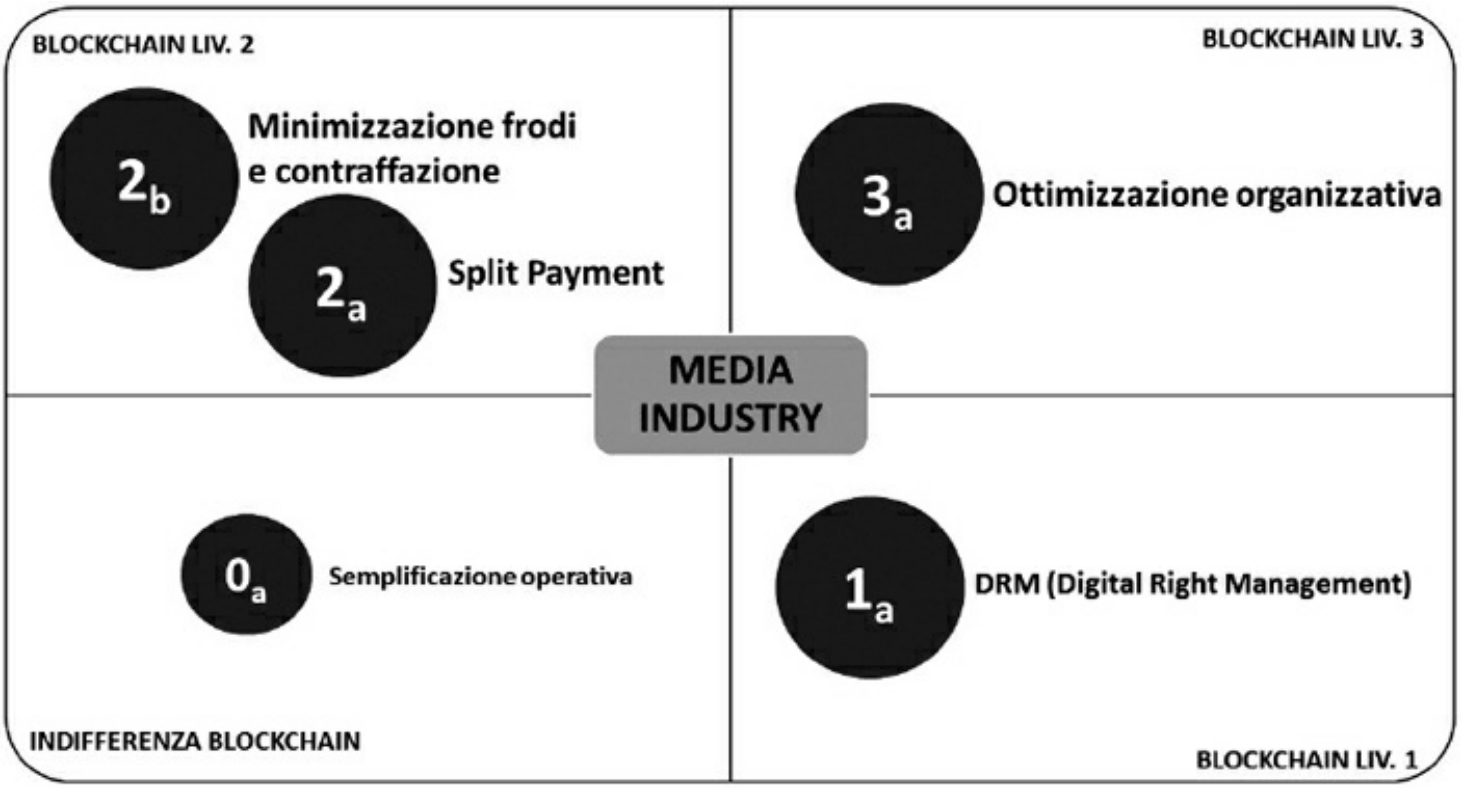

Figura 22.8 – Benefici DLT per Media industry.

Settore pubblico

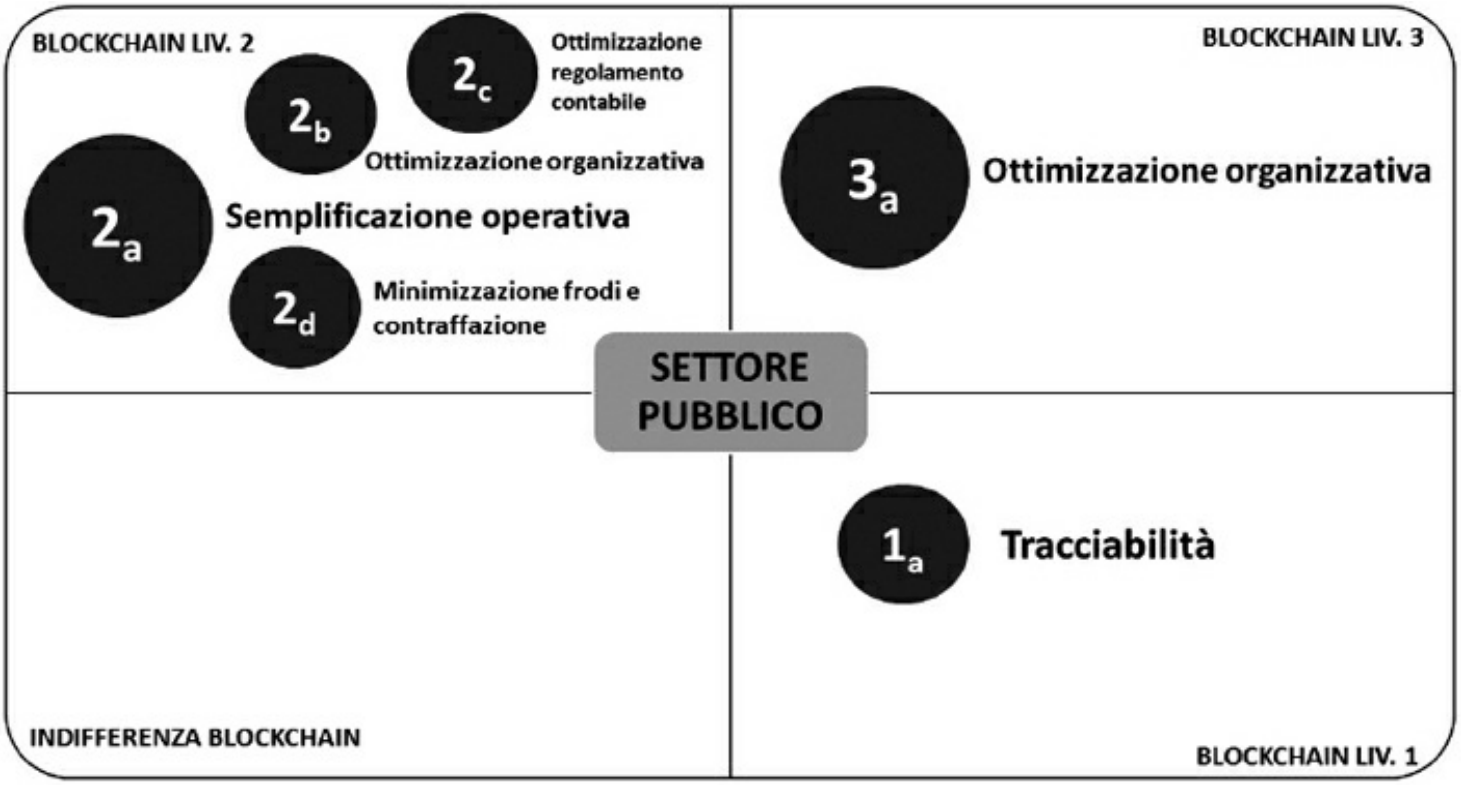

Figura 22.9 – Benefici DLT per Settore pubblico.

Sharing economy

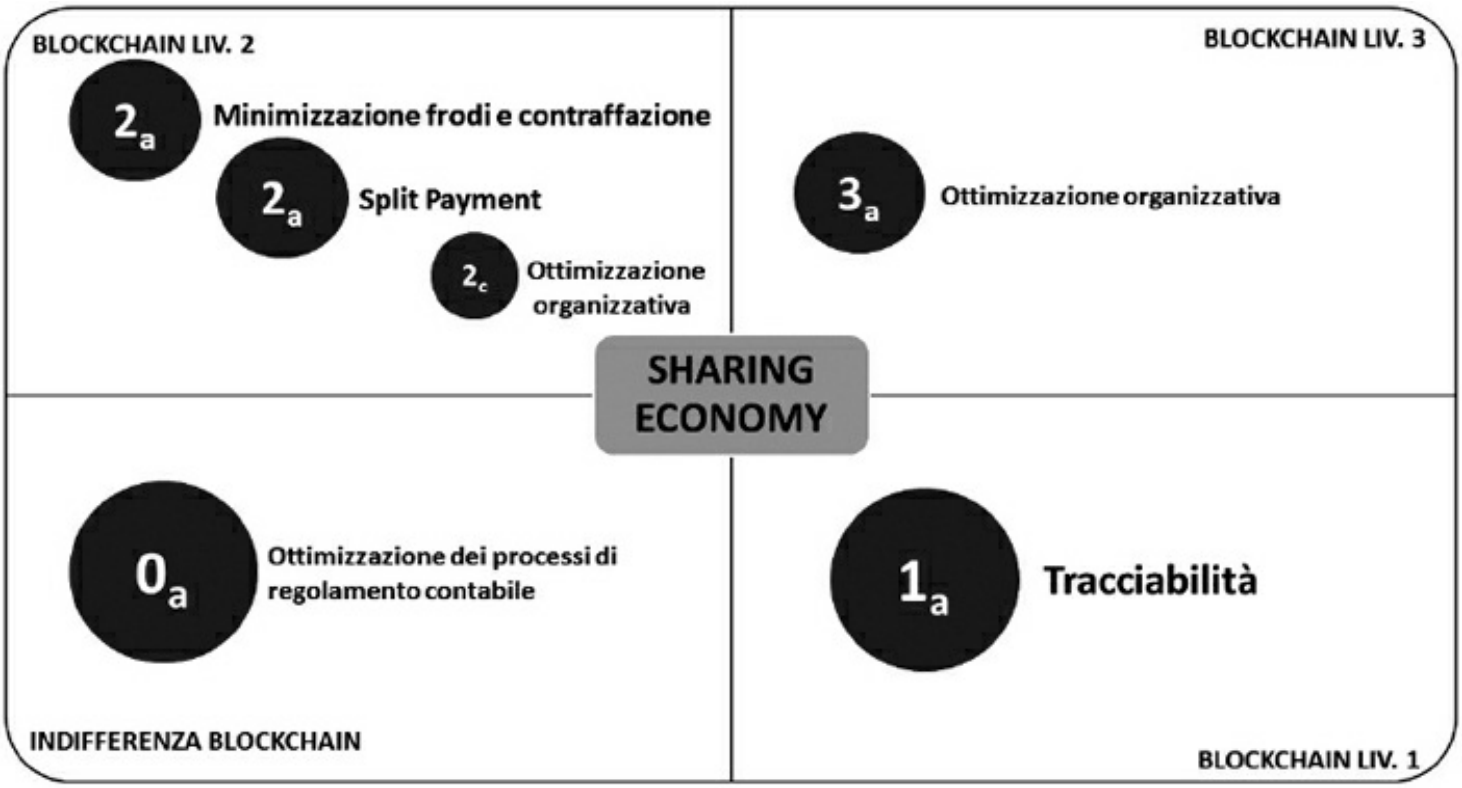

Figura 22.10– Benefici DLT per Sharing economy.

Trasporti

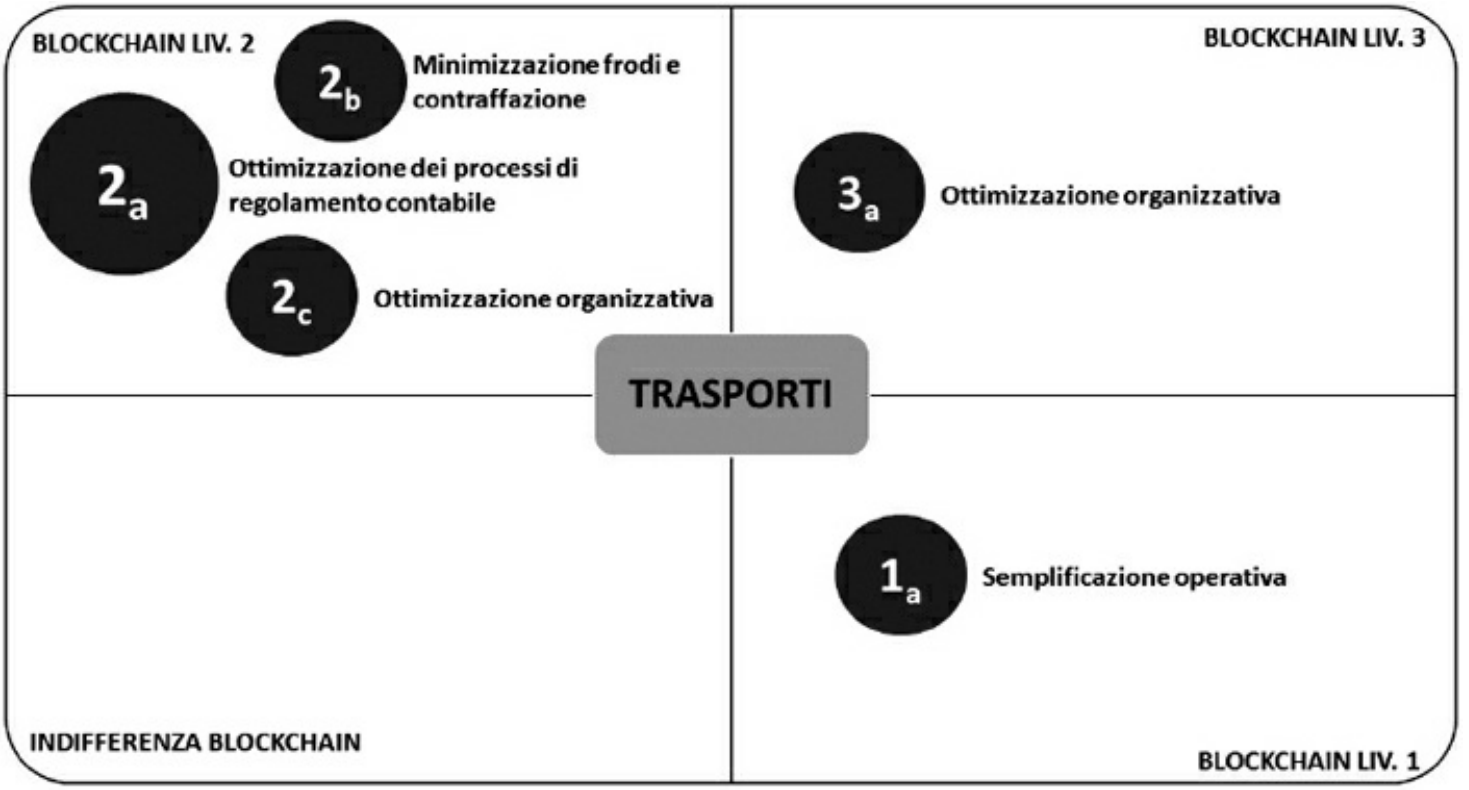

Figura 22.11 – Benefici DLT per Trasporti.

Turismo

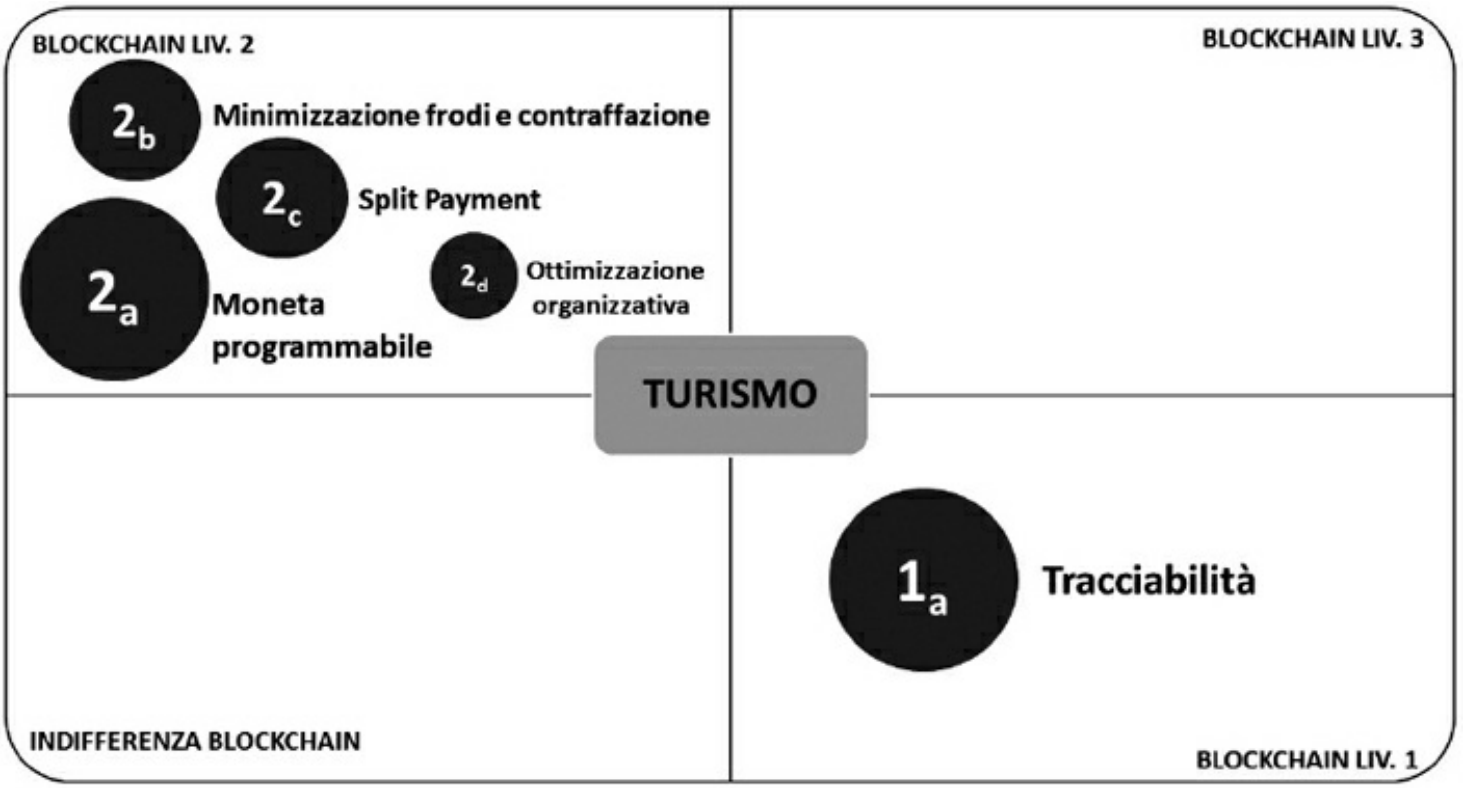

Figura 22.12 – Benefici DLT per Turismo.

Utilities

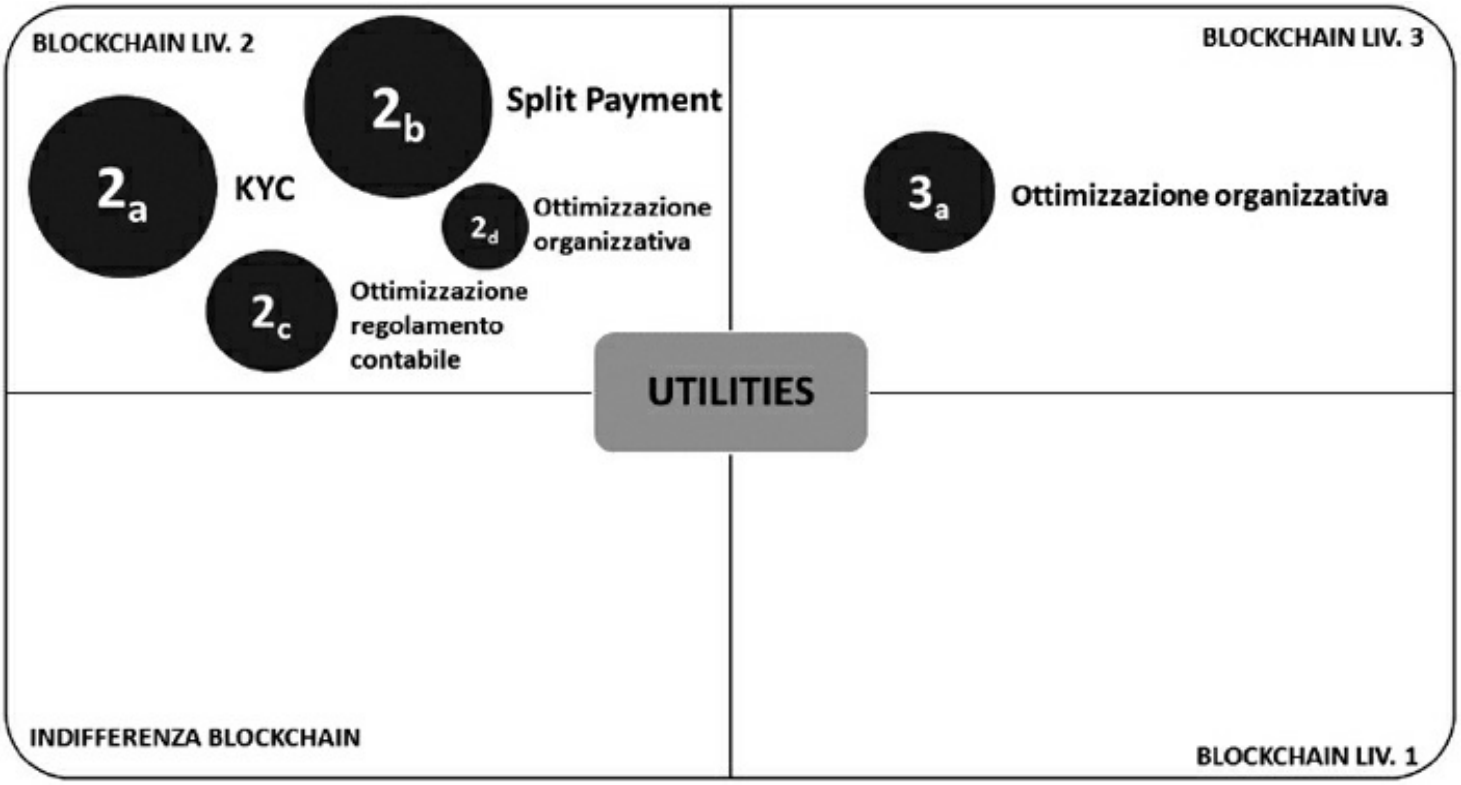

Figura 22.13 – Benefici DLT per Utilities.

Welfare

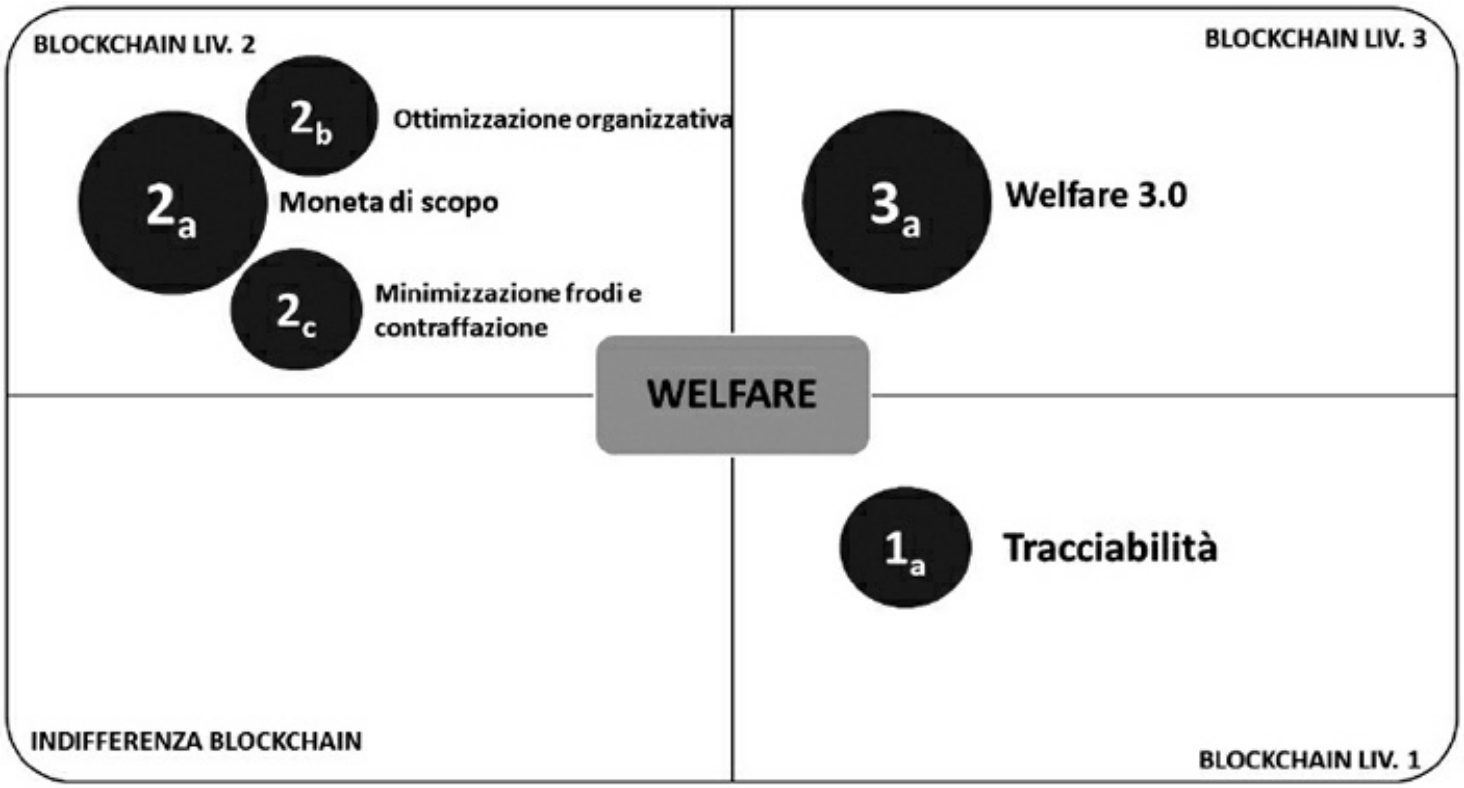

Figura 22.14 – Benefici DLT per Welfare.

PARTE VI
SCENARI E STRATEGIE

Ogni progresso della civiltà
è stato denunciato come innaturale
quando era ancora recente.

Bertrand Russell

23

Scenari

Siamo quasi giunti al termine di questo libro e, dopo avervi spiegato ciò che è stato, che è e che potrebbe essere la blockchain, proiettiamoci in un orizzonte temporale compreso fra i 2 e i 20 anni e proviamo a immaginare quali potranno essere gli scenari di sviluppo di questa tecnologia. Ma prima di alzare troppo presto lo sguardo ci sono ancora due

questioni che dobbiamo sviluppare.

La prima arride alla Blockchain con la "B" maiuscola (quella dei Bitcoin e delle Proof-of-Work) ed è ciò che ormai avrete ben compreso: trovare una soluzione di compromesso per renderla più scalabile evitando il ricrearsi di pericolose "concentrazioni di fatto". Forse una soluzione c'è e, sebbene ancora *in nuce*, è opportuno considerarla, si chiama Lightning Network.

Il secondo tema che non abbiamo ancora trattato, per quanto possa sembrarvi assurdo è la blockchain... senza il bisogno di una blockchain; si chiama IOTA ed è davvero entusiasmante. Ma procediamo con

ordine; diamo subito una rapida sintesi di Lightning Network e spieghiamo quali siano le straordinarie opportunità che da tale sistema possono schiudersi.

Che cos'è il Lightning Network

Immaginiamo che sulla Blockchain dei Bitcoin non tutte le transazioni debbano necessariamente essere registrate e che alcune di esse possano essere regolate all'esterno, ossia "off-chain". In che modo? Aprendo dei canali tra mittente e destinatario della criptovaluta e notarizzandone l'evento sulla Blockchain. Questa transazione di

“apertura” viene registrata irreversibilmente sul Distributed Ledger in modo che non possa essere disconosciuta e, per dare “sussistenza” alla prova, entrambi i partecipanti congelano una propria disponibilità di criptoasset, che resterà a garanzia delle successive transazioni. Gli scambi che avverranno finché il canale rimane aperto saranno tutti “off-chain” e potranno così essere velocizzati laddove non vi sarà la necessità di minarne i blocchi. Alla chiusura del canale si fanno i conti e avviene ciò che tecnicamente si chiama compensazione, ossia i due saldi precedentemente congelati sono compensati sulla base

delle posizioni debitorie e creditorie finali venutesi a costituire con le transazioni "off-chain". Seguendo questa logica è possibile creare dei canali fra più coppie mittente/destinatario, in modo da creare una rete alternativa, ed è su questa rete separata dalla Blockchain che può svilupparsi un'economia di scambi basata sulle promesse di disponibilità dei criptoasset. Scambiando "promesse" off-chain non si incorre nei cali prestazionali tipici delle transazioni on-chain ma, ovviamente, è necessario dare un valore a queste promesse di disponibilità, un valore che dovrà essere sempre garantito dai depositi di criptoasset rilasciati nel momento in cui viene registrata

l'apertura dei canali.

I pregi dovrebbero esservi a questo punto già molto chiari ed evidenti. Quali possano essere i difetti forse meno. Se da un lato, infatti, la Blockchain potrebbe essere più scalabile mantenendo le proprie caratteristiche di base pressoché integre, il rischio di ricostituire un Trent centrale (per ritornare alla nostra metafora di Welthyland) nella figura (o nelle figure) di pochi possessori di enormi disponibilità in criptoasset, che possono quindi permettersi di congelare ingenti quantità e non chiudere mai i canali, si ripropone con le stessa rischiosità rappresentata dai mining pool di cui

abbiamo parlato nel paragrafo “Bitcoin Gold” (Capitolo 12).

La strada da percorrere è ancora lunga, ma c’è già chi pensa di applicare regole condivise per cui un singolo non possa tenere aperto il canale più di un certo tempo o possa farlo solo se consuma esso stesso su quel canale una propria effettività disponibilità di criptoasset, limitata preventivamente sulla base di un accordo validato sulla Blockchain.

Nell’attesa di comprendere se questa strada porterà davvero a dei risultati apprezzati collettivamente, affrontiamo il “nuovo che avanza” e parliamo di IOTA.

Che cos'è IOTA

L'assonanza con il termine IoT (Internet-of-Things) è piuttosto evidente. Stiamo infatti parlando della miriade oceanica di oggetti (o se preferite di dispositivi) più o meno intelligenti, connessi a Internet, che gli analisti stimano per la prossima decade superare i 50 miliardi di unità. Questi dispositivi – pensate per esempio ai sensori – non sono sfruttati appieno nella loro straordinaria potenza, poiché restano molto spesso inattivi (pur mantenendo aperta la connessione alla rete) e prestano il loro servizio solo nei momenti che coincidono con il verificarsi di particolari eventi. L'idea di chi ha progettato IOTA[101] nasce

proprio da una considerazione economica degli oggetti, o meglio, dell'economia degli oggetti: rendere disponibile il surplus inutilizzato a chiunque ne abbia necessità. In tal modo, gli oggetti interconnessi diventano una sorta di backbone in grado di servire coloro che, per scopi diversi, hanno l'esigenza di comunicare, di interagire e, perché no, di scambiare valore. Immaginiamoci IOTA come una specie di marketplace dove chiunque può accedere acquistando servizi di interscambio, sfruttando così una rete di dispositivi che può essere remunerata. Remunerazione è un termine che abbiamo già abbondantemente

assimilato nella lettura di questo libro; sappiamo dunque capire che, per quanto "smart" possano essere questi terminali IoT, ben difficilmente accetteranno i Bitcoin; men che meno potranno pensare di riuscire a minare le transazioni in qualsiasi altra criptovaluta tra quelle che abbiamo fin qui descritto, perché gli sforzi richiesti da qualsiasi protocollo di consenso distribuito non consentirebbero loro alcuna chance. Ed è qui che l'intuizione del creatore di IOTA si sviluppa. Invece di pensare a un sistema di basato su algoritmi ad alto consumo di risorse, pur mantenendo valido il concetto di consenso distribuito, nasce il Tangle. Basato su un protocollo software a grafici aciclici

diretti, con il Tangle le transazioni vengono processate in parallelo; ciò consente a IOTA di scalare in maniera direttamente proporzionale alla crescita del network. IOTA usa firme crittografiche Hash-based anziché crittografia a curva ellittica (come quelle impiegate per i Bitcoin), che offrono maggior velocità e semplicità nella verifica dei dati, riducendo la complessità del Tangle e azzerando qualsiasi costo di gestione delle varie azioni (altro che Gas di Ethereum!).

Inoltre, differentemente da quanto avevamo visto per le blockchain che prevedono un asset nativo, l'emissione di Tangle è già avvenuta unitariamente

al momento del lancio di IOTA. Non esiste neppure il concetto di ricompensa. Quando un utente sottopone una transazione all'approvazione del network, si assume anche l'approvazione di altre due transazioni scelte casualmente; ciò permette di evitare il ricorso a qualsiasi nodo validatore, velocizzando i tempi per confermare l'esito della transazione. Una transazione che, avrete già capito, non è solo in IOTA (anzi MIOTA, così si chiama il criptoasset), ma può accompagnare anche qualsiasi altro dato.

I maggiori limiti delle

blockchain

Alla luce di quanto vi abbiamo sin qui descritto, prendendo anche in considerazione le nuove opportunità che Lightning Network e IOTA rappresentano, per quanto ancora molto *still in its infancy*, proviamo a riassumere i limiti delle blockchain per come le abbiamo analizzate. Ciò ci consentirà di capire in quali termini la ricerca dovrà svilupparsi, dovendosi focalizzare sul superamento degli ostacoli opposti.

Centralizzazione del

controllo

La capacità computazionale dei miner può tendere a concentrarsi nei cosiddetti "mining pool", ossia gruppi di server particolarmente costosi che sono installati e operativi in quei Paesi dove, sfruttando il basso costo dell'energia elettrica, è possibile detenere una potenza di calcolo maggiore. Una concentrazione siffatta mette fuori gara chi non ha a disposizione elevate risorse per competere. Esiste dunque un possibile rischio che tale concentrazione conferisca un potere eccessivo a un gruppo limitato di nodi, insidiando il principio di base della Blockchain,

ossia la decentralizzazione dei controlli basata su un modello di governance distribuita.

Crittografia quasi obsoleta

La crittografia alla base di molte blockchain è in alcuni casi a severo rischio di obsolescenza. Pertanto, è ragionevole pensare che con il passare degli anni una potenza di calcolo sempre più "disponibile" possa rendere estremamente vulnerabili i sistemi di sicurezza attuali. Sebbene i calcolatori quantistici non siano ancora prodotti di

consumo, è forse utile iniziare a progettare nuove soluzioni che siano *quantum-resistant* sotto il profilo crittografico.

Gestione delle Fork

Nei casi di Hard Fork che abbiamo descritto nel paragrafo "Le Fork sulla Blockchain" (Capitolo 12), o meglio durante il propagarsi degli effetti sul network di una Hard Fork, emergono alcuni rischi che pongono in pericolo l'affidabilità e, soprattutto, l'immutabilità delle transazioni avvenute. Ciò che infatti può accadere è il manifestarsi dei cosiddetti "replay

attack", dove soggetti malintenzionati replicano le transazioni, appena effettuate sulla catena di origine, sulla nuova catena. Ciò evidenzia una vulnerabilità endogena delle blockchain permissionless e, più in generale, dei modelli di DLT che sfruttano i protocolli di una blockchain pubblica.

Separazione dei ruoli tra i partecipanti a una blockchain

Le blockchain che si basano su un asset nativo negoziabile sono sistemi eterogenei con nette separazioni dei

ruoli (miner più potenti, miner meno potenti, semplici utenti) che possono innescare discriminazioni e accendere conflittualità (si veda a tal riguardo anche il box del Capitolo 12 "I vulnus della e-democracy").

Limiti di scalabilità

In fase di progettazione di nuove blockchain che prevedono limiti alla gestione delle transazioni (come è il caso dei Bitcoin) è sempre necessario ricordare che è molto complesso stimare con precisione i valori di detti limiti, che saranno ideali solamente quando il sistema sarà in esecuzione alla sua

massima capacità.

Consumo energetico

È probabilmente uno degli aspetti più importati da considerare se si pensa che calcoli approssimativi ci dicono che la rete di computer del sistema Bitcoin usa 3,4 gigawatt.

Guardiamo più in là…

È giunto dunque il momento di provare a immaginare i possibili scenari di sviluppo di questa tecnologia, che vi abbiamo raccontato nei suoi pregi e difetti. La Tabella 23.1 vi propone, in un

arco temporale suddiviso per tre differenti profondità, alcune riflessioni.

Profondità temporale	**Scenari**
Medio termine (2-5 anni)	• Sviluppo soluzioni "Lightning Network" like • Interoperabilità tra blockchain private • Interoperabilità tra blockchain pubbliche • Interoperabilità tra blockchain private e blockchain pubbliche • Sviluppo di sidechain • Evoluzione linguaggi di scripting • Interazione con oggetti interconnessi (IoT e IoeT) • Regolamentazione ICO • Regolamentazione impieghi blockchain per settori di competenza • Regolamentazione DAO
Medio-lungo (5-10 anni)	• Blockchain-as-a-services

	• Nuove blockchain e DApp su piattaforme pubbliche • Pervasività blockchain per IoT • Regolamentazione DAO • Implementazione nuove DAO in ambito istituzionale
Lungo termine (10-20 anni)	• DAO di oggetti • Modelli di apprendimento e studio DAO • Etica DAO • Arte e cultura DAO • Continenti DAO

Tabella 23.1 – Ipotesi di scenari.

---

101. L'ideatore di IOTA è il programmatore David Sønstebø.

Smitizziamo le blockchain

Stiamo per congedarci. Prima di lasciare ognuno di voi alle riflessioni che riterrà più opportune e utili (noi auspichiamo sempre finalizzate al conseguimento di obiettivi perseguibili e sostenibili), vogliamo consegnarvi qualche pillola di sana obiettività. Le

migliori strategie si progettano esercitando consapevolmente un pensiero laterale, ma affrancandosi dalle fascinazioni di ciò che appare innovativo. La trappola dei bias cognitivi (specie quelli di conferma) è sempre innescata e occorre stare bene all'erta. Eccovi qualche suggerimento.

- **Le blockchain sono sempre "trustless"**

  Le blockchain richiedono un certo grado di fiducia nel sistema di crittografia (sempre e in ogni caso). In particolare:

  – nel caso di blockchain permissioned, la fiducia deve essere riposta in chi

identifica e preseleziona i validatori (oltre che nei validatori, ovviamente);

- nel caso di blockchain permissioned, la governance del sistema richiede sempre una terza parte fidata.

- **Le blockchain garantiscono sempre l'immutabilità**

  In alcune circostanze ciò potrebbe non essere sempre garantito:

  - nel caso di attacchi del 51% per le blockchain permissionless;

- teoricamente nelle blockchain permissioned il rischio è maggiore laddove il numero di validatori fosse inferiore a quello delle blockchain permissionless, poiché la facilità di colludere sarebbe maggiore;
- nelle blockchain permissioned, però, la garanzia che una collusione tra validatori non avvenga è dipesa dagli obblighi scritti in un accordo con validità legale.

- **Le blockchain posseggono la verità assoluta e sono giudici universali**

  Questo non è universalmente vero e bisogna riflettere sulle diverse tipologie di token:

  – i *fiat* Pegged Token e gli asset Backed Token hanno sempre un rapporto con il mondo esterno alla blockchain e bisogna fare i conti con la convertibilità dei diritti che essi rappresentano nel momento in cui li si vuole riconosciuti anche nel mondo esterno;

– gli Utility Token, nel perimetro della loro mera funzionalità tecnica, sono certamente più garantiti.

Appendice

Valute digitali

Per spiegare che cosa siano le valute digitali, è opportuno definire una tassonomia. Nella Figura A.1 ne vediamo una organizzata seguendo una rappresentazione piramidale.

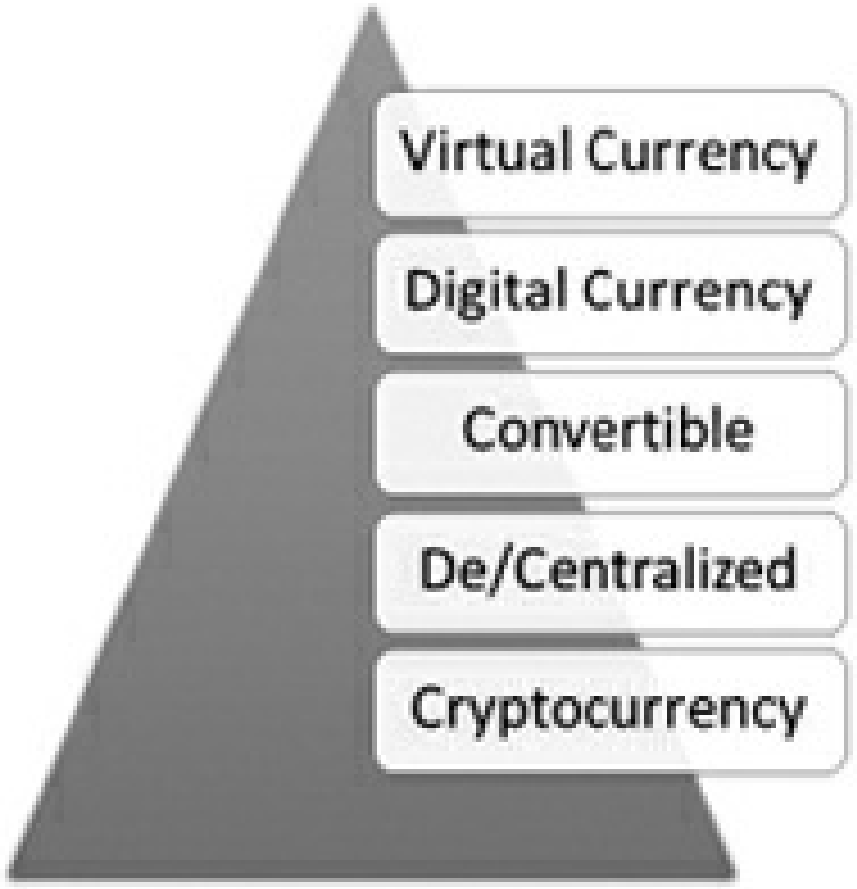

Figura A.1 – Tassonomia delle valute digitali.

Che cosa sono le Virtual Currency

Le Virtual Currency:

- sono rappresentazioni digitali

di valore, utilizzate, su base volontaria, come mezzo di scambio per l'acquisto di beni e servizi;

- possono essere trasferite, conservate e negoziate elettronicamente;
- non hanno corso legale e pertanto non devono per legge essere obbligatoriamente accettate per l'estinzione delle obbligazioni pecuniarie. Possono essere utilizzate per acquistare beni o servizi solo se il venditore è disponibile ad accettarle[102].

Che cosa non sono le Virtual Currency

Le Virtual Currency:

- non sono emesse da banche centrali o da autorità pubbliche;
- non rappresentano in forma digitale le comuni valute a corso legale (Euro, Dollaro ecc.);
- non costituiscono moneta legale;
- non sono assimilabili alla moneta elettronica[103], le cui transazioni hanno, invece,

valore liberatorio.

Che cosa sono le Digital Currency

Le Digital Currency sono una rappresentazione digitale:

- di Virtual Currency (non *fiat*);
- di "moneta *fiat*", ossia di moneta elettronica[104].

La convertibilità delle Virtual Currency

Classificando le Virtual Currency in

relazione all'interazione con la moneta a corso legale (ossia la "moneta *fiat*"), la Banca Centrale Europea ha definito una matrice che riportiamo in Figura A.2, estratta dal documento "Virtual Currency Schemes" edito dalla BCE nel mese di ottobre 2012.

La colonna referenziata come "Type 1" rappresenta una Virtual Currency che non è mai convertibile (a titolo esemplificativo le "miglia" di un programma di fidelizzazione per frequent flyer appartengono a tale tipologia). Le colonne referenziate con "Type 2" e "Type 3" rappresentano una Virtual Currency convertibile; per esempio le valute virtuali adottate

all'interno di giochi MMORPG[105] sono rubricabili nella seconda colonna della matrice, mentre i Bitcoin si ascrivono nella classificazione indicata dalla terza colonna.

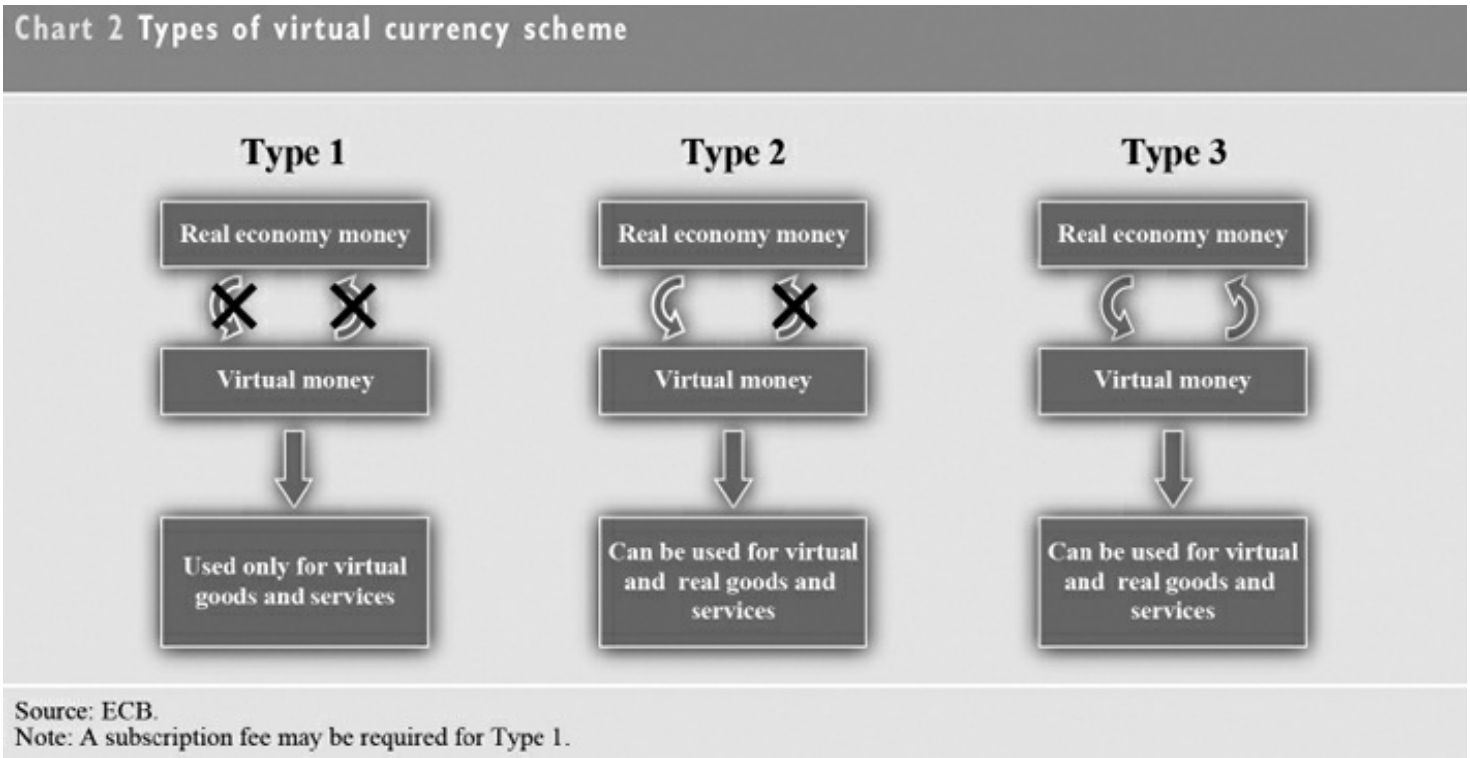

Figura A.2 – Tipologie di Virtual Currency in relazione alla loro convertibilità in moneta a corso legale.

L’emissione di Virtual Currency

Classificando le Virtual Currency in relazione alla loro emissione possiamo avere due tipologie, come riportate nella Tabella A.1.

Emissione			
Centralizzata	Sono emesse da un singolo “Scheme Owner” (Autorità Centrale) che può: • amministrare l’emissione di una Virtual Currency; • stabilire le regole di utilizzo della Virtual Currency; • Gestire il libro mastro (il c.d. “Payment Ledger”) delle transazioni effettuate con la Virtual Currency; • possedere l’autorità di ritirare la Virtual Currency in circolazione in qualsiasi momento; • definire le regole di cambio (fisso o variabile) della Virtual Currency contro moneta a corso legale.	**Decentralizzata**	Non esiste uno “Scheme Owner” centrale, perciò: • non esiste un soggetto amministratore vigilato; • non esiste un’Autorità Centrale; • il libro mastro (il c.d. “Payment Ledger”) delle transazioni è distribuito (“Distributed Payment Ledger”); • il funzionamento è basato su sistemi: distribuiti, open source, operativi su reti Peer-to-Peer.

Tabella A.1 – Classificazione delle Virtual Currency in relazione all’emissione.

Che cosa sono le Cryptocurrency (o criptovalute)

Le Cryptocurrency sono valute virtuali digitali emesse in modo decentralizzato (non esiste uno Scheme Owner centrale) per le quali:

- il "libro mastro" è pubblico ("Distributed Ledger") e contiene tutte le transazioni effettuate;
- la validazione del "libro mastro" viene eseguita a intervalli di tempo (per esempio ogni 10 minuti)

tramite una rete Peer-to-Peer e mediante l'implementazione di algoritmi crittografici (durante l'effettuazione di altre transazioni) secondo un protocollo chiamato "Blockchain";

- durante la validazione del "libro mastro" sono coniate nuove unità di Cryptocurrency (sistema di remunerazione che ripaga – almeno in parte – il costo di emissione).

---

102. Il valore liberatorio del pagamento in moneta a corso legale stabilito dall'art. 1277 c.c.

103. La moneta elettronica è definita nel T.U.B. (Testo Unico Bancario di cui al d.lgs. 1° settembre 1993, n. 385) all'art. 1, comma 2, lettera h-*ter*.

104. Vedere la nota precedente.

105. Massively Multiplayer Online Role-Playing Game, ovvero giochi di ruolo per computer o console che vengono svolti tramite Internet contemporaneamente da più persone reali.

Glossario

Address: coincide con la chiave pubblica di un wallet ed è formata da una stringa di caratteri alfanumerici utilizzata per ricevere o inviare le transazioni.

Blocco: è un raggruppamento di transazioni verificate ed è un'unita di cui si compone la Blockchain che contiene

tutte le transazioni verificate durante il periodo di generazione del blocco stesso; mediamente ogni 10 minuti viene generato un nuovo blocco e aggiunto in modo cronologico alla catena di blocchi.

BTC: è l'abbreviazione di Bitcoin, l'asset nativo della Blockchain.

Chiave privata: è una chiave crittografica utilizzata in un sistema di crittografia asimmetrica e deve essere custodita gelosamente; nel sistema Bitcoin la chiave privata si compone di un codice alfanumerico associato a ogni wallet.

Chiave pubblica: è una chiave

crittografica utilizzata in un sistema di crittografia asimmetrica che può essere scambiata anche su un canale non sicuro; nel sistema Bitcoin la chiave pubblica è rappresentata dall'Address.

Criptoasset: è l'asset nativo di una blockchain (nella Blockchain è costituito dai Bitcoin).

Difficoltà: rappresenta la misura di quanto sia complicato trovare un Hash al di sotto di un certo target. Nella Blockchain dei Bitcoin non può essere inferiore a 1 e viene aggiustata ogni 2.016 blocchi, ossia mediamente ogni 12 giorni; è un valore inversamente correlato con il Target e positivamente correlato con l'Hash rate.

ETH: è l'abbreviazione di Ether, l'asset nativo della blockchain di Ethereum.

Firma digitale: si tratta di un processo crittografico basato su chiavi asimmetriche che, insieme alla funzione di Hash, permette di provare che una transazione in criptoasset sia generata da chi realmente è in grado di accedere al proprio wallet.

Hash: la funzione di Hash è un sistema matematico che consente di convertire un messaggio di lunghezza arbitraria in un messaggio in codice alfanumerico di lunghezza fissa o prefissata.

Ledger: è il registro pubblico distribuito (Distributed Ledger) nel

quale vengono “annotate” con la massima trasparenza tutte le transazioni effettuate in modo ordinato e sequenziale. Il ledger è costituito da una serie di blocchi che sono tra loro incatenati mediante una funzione crittografica e l’uso di Hash.

Mance (o commissioni): donazioni, liberamente incluse nelle transazioni su iniziativa dei singoli, che i miner possono incassare a lavoro di validazione compiuto (servono da incentivo per i miner).

Miner: nella Blockchain un miner è un nodo validatore dei blocchi.

Mining: nella Blockchain è il processo

con cui si validano e registrano le transazioni.

Moneta *fiat*: è sinonimo di valuta a corso forzoso o valuta legale.

Network: è il sistema che rappresenta la blockchain, organizzato in nodi secondo una rete che può essere distribuita, decentralizzata e paritaria (il network Bitcoin è costruito su un sistema di tipo Peer-to-Peer).

Nodo: i partecipanti alla blockchain vengono chiamati nodi; sono costituiti fisicamente da server mediante i quali vengono gestite le transazioni in criptoasset.

Nonce: è una stringa casuale di dati che

viene utilizzata nel processo di hashing di un blocco; viene utilizzato un nonce diverso per ogni tentativo di hashing, al fine di soddisfare il target richiesto nel processo di mining di un blocco.

Proof-Of-Work (PoW): nella Blockchain dei Bitcoin è la prova che consente ai miner di dimostrare a tutti gli altri nodi la validazione del blocco e che permette loro di ottenere la ricompensa (più le eventuali mance).

Protocollo: nella Blockchain il protocollo rappresenta l'insieme di regole condivise da tutti i nodi che, essenzialmente, definiscono: la dimensione dei blocchi, come deve essere raggiunto il consenso distribuito,

la politica di incentivazione e remunerazione dei miner, la variazione dei livelli di difficoltà.

Reward (o ricompensa): nella Blockchain costituisce la remunerazione dei miner in criptoasset.

Target: è un numero estremamente grande (a 256 bit) il cui valore si modifica in base al tempo effettivo e teorico necessario per validare 2.016 blocchi.

Transazione: uno scambio di criptoasset tra due o più nodi si chiama genericamente transazione.

Transazione confermata: è una transazione verificata che si trova in un

blocco validato distante dall'ultimo blocco validato di almeno 5 posizioni. Nel sistema Bitcoin, poiché mediamente ogni 10 minuti viene validato un blocco e aggiunto alla catena, si ha una transazione confermata ogni 60 minuti.

Transazione validata: è una transazione verificata che si trova in un blocco validato.

Transazione verificata: è la singola transazione verificata dai nodi partecipanti.

Wallet: è un portafoglio elettronico che memorizza tutte le credenziali per accedere, spendere e trasferire criptoasset su una blockchain.

Informazioni sul Libro

- Caratteristiche delle blockchain
- Ambiti applicativi
- Scenari
- Strategie di sviluppo

Come funziona la Blockchain? Come si lavora con i protocolli del consenso distribuito e gli Smart Contract? Quale futuro emergerà dal mondo delle criptovalute?

Il libro risponde a queste e a molte altre domande, illustrando a fondo le principali architetture basate su Distributed Ledger oggi disponibili e spiegando in quali aree cross-industry avranno maggiori possibilità di imporsi. Il volume analizza inoltre le strategie di sviluppo che nei prossimi anni potrebbero essere adottate da aziende private, pubbliche e dalle istituzioni, per cogliere i maggiori vantaggi e ridistribuirli a beneficio di una più ampia comunità.

Per capire la Blockchain occorre innanzitutto non confonderla con i Bitcoin, avere chiare le caratteristiche che la rendono unica e comprenderne gli

effettivi vantaggi. L'opera illustra pertanto gli ambiti che possono trarre un reale profitto dall'adozione di soluzioni basate su questa piattaforma, altri per i quali può essere ininfluente, altri ancora in cui provocherebbe impatti negativi. Analizza infine tutti gli aspetti che possono determinare il successo o il fallimento di un progetto innovativo, special-mente per chi pensa di investire nel cambiamento portato dalle blockchain.