La guida strategica che spiega ad imprenditori e manager come sfruttare la tecnologia che cambierà il mondo.

FARE Business CON LA Blockchain

Enrico Talin

Commerc.io

Ai miei genitori che mi hanno insegnato a dare valore alle cose.

A mia moglie da cui ho imparato a non darci troppo valore.

A mio figlio a cui sto insegnando a dare il giusto valore alle cose.

Enrico Talin

Titolo: **Fare Business con la Blockchain**

ISBN: 9788885623071

Published by **Tradenet Services Srl Editore** (IT)

Giugno 2019: **Prima edizione**

Grafica ed illustrazioni:
Nextindustry.net

Commerc.io S.r.l. e sono riservati all'utilizzo di Commerc.io S.r.l. e/o dei suoi aventi causa debitamente autorizzati e

sono protetti dalle leggi nazioni e internazionali in materia di tutela della proprietà intellettuale e industriale. L'utilizzo

da parte di terzi di trade name, loghi, simboli, slogan, qui indicati, in qualsivoglia forma e modalità effettuato, se non

preventivamente autorizzato da Commerc.io S.r.l. verrà perseguito a norma di legge.

AVVERTENZE

Le informazioni contenute in questo volume relative alla rete di Commercio.Network non hanno carattere esaustivo

e non devono essere intese quale offerta o promessa al pubblico. I Network upgrades successivi alla versione 1.0 sono

in fase di sviluppo. Il contenuto del presente volume non può essere inteso come un impegno di Commerc.io S.r.l. a

completare tale sviluppo e/o ad assicurarne funzionalità, risultati o vantaggi economici e non.

Tradenet Services Srl Editore

Via G. Marconi, 3

36015 Schio (VI)

Tel. 0445. 57.53.99

www.tradenet.it

Printed in Italy

Finito di stampare nel mese di giugno 2019 presso tipografia **Grafiche Stella Srl** - San Pietro di Legnago - Verona - Italy

Un grande ringraziamento ai miei compagni di viaggio sul a Blockchain

che hanno permesso la realizzazione di questo libro:

DAVIDE COLETTO

ENRICO GIACOMELLI

LEANDRO PRAI

FRANCESCA MORIANI

ANTONIO GENTILE

ALBERTO BORTOLETTO

MATTEO CAVALCANTE

ALESSANDRO BORTOLETTO

FILIPPO MOOR

FEDERICO STEGAGNO

ENRICO MAZZOCCO

GIANLUCA LANZA

MAURIZIO MALAMAN

PAOLO FIORAVANTI

FEDERICO FALIVA

STEFANO VISONA'

JOHNNY MALAMAN

ANTONIO LANZA

CLAUDIO MALAMAN

DAVINO CIAMPELLI

ANDREA FIORAVANTI

MIRKO GATTO

ENRICO CHECCHIN

MIRKO DA CORTE

GIORGIO BORGOGNO

SERGIO MARCHESE

ROY REALE

FARE **Business** CON LA **Blockchain**

La guida strategica che spiega ad imprenditori e manager

come sfruttare la tecnologia che cambierà il mondo.

Enrico Talin

commerc.io

Citazioni

8

Capitolo terzo

72

Blockchain 1.0: Bitcoin

20

Utility Token

80

Blockchain 2.0:Ethereum

21

Non-Fungible Token (NFT)

81

Blockchain 3.0:network di Blockchain

30

indice generale

Citazioni

8

“Whereas most technologies tend to automate workers on

“Blockchain is like the new big data or AI - too many people

the periphery doing menial tasks, blockchains automate

are using it as a buzzword and not focused solving a real

away the center. Instead of putting the taxi driver out of

problem. We like to call them Blockchain tourists!”

a job, blockchain puts Uber out of a job and lets the taxi

Brad Garlinghouse

drivers work with the customer directly.”

Vitalik Buterin

“In the blockchain world, each user can and should own

their data, and ‘central’ players are less vulnerable to data

“Everything will be tokenized and connected by a

losses and breaches.”

blockchain one day.”

William Mougayar

Fred Ehrsam

“There is an opportunity to recreate the financial world as

“The blockchain does one thing: It replaces third-party trust we know it in

the parallel universe that is the blockchain.

with mathematical proof that something happened."

We are writing rules for this whole new universe."

Adam Draper

Patrick M. Byrne

"The blockchain symbolizes a shift in power from the centers "Blockchain is really exciting technology because it's

to the edges of the networks."

actually providing both transparency but also agility in a

William Mougayar

contractual relationship that any organization should have.”

Jean-Philippe Courtois

Capire cos'è una Blockchain non è facile: occorre capire il suo messaggio per poterne apprezzare il potenziale.

Al di là dell'aspetto tecnologico, una Blockchain porta con sé dei fondamentali filosofici, culturali e ideologici che

devono essere assolutamente compresi.

Una cosa è certa: la Blockchain è una rivoluzione, è un cambio di paradigma che avviene in media solo ogni decina di anni.

Anni 70

Anni 80

Anni 90

Anni 00

Anni 10

Anni 20

Mainframe

PC

Internet

Social

Mobile

Blockchain

12

Guardando al passato possiamo notare che ogni nuovo Il resto del libro affronta l'aspetto funzionale ed è un viaggio

paradigma ha soppiantato quel o del periodo precedente. che apre un mondo di potenzialità oltre ogni immaginazione.

Appare dunque fondamentale conoscere e comprendere a In questo libro vogliamo insegnarvi a camminare nel sentiero

fondo la prossima tecnologia emergente per non subirla.

del a Blockchain, ma sarete voi a decidere che autostrade

La storia ci insegna che molte aziende sono state superate percorrere e che posti visitare. Solo voi conoscete la vostra

da altre perché non sono riuscite a sfruttare le opportunità azienda o i suoi processi di business, e solo voi sarete in grado

di questi cambi di paradigma.

di capire come utilizzare la Blockchain, dopo aver imparato

Una Blockchain non è un'App o un

software da instal are e cosa fare con essa. Ovviamente al ’inizio faremo un po’ di

usare in uno smartphone o su un computer.

strada insieme per ambientarci, ma poi vi muoverete da soli.

Una Blockchain è una tecnologia abilitante che permette

di fare qualcosa in un modo completamente diverso

rispetto a prima, nello stesso modo in cui oggi mi collego

sul web per prenotare una stanza in un hotel dall'altra

parte del mondo e per farlo non è necessario utilizzare il

fax o il telex.

Appena compreso il concetto di Blockchain, un'azienda non

può più fare a meno di iniziare ad immaginare che cosa possa

fare per diventare più competitiva con essa.

L'aspetto tecnologico trattato nel primo capitolo è il più

complesso di questo libro, quindi anche se non viene

completamente compreso, i concetti di base vengono

ripetuti più volte nei capitoli successivi.

13

Approfondimenti

Come fare per leggere gli approfondimenti:

Scrivere un libro su una materia che cambia minuto per

minuto è abbastanza complesso.

Abbiamo pensato di creare ***1) Scaricare un' app che riconosce i QR Code (basta cercare***

un sito chiamato
Blockchainworkshop.it

"QR Reader" sullo store Apple o Google.

per tenersi aggiornati con una serie esclusiva di ***2) Inquadrare il QR code presente sulla pagina con lo smart***

approfondimenti e notizie.

Phone.

La freccia verde che contiene un QR

Code è un link a una ***3) Visitare il sito per leggere gli approfondimenti (video,***

pagina web disponibile ai lettori del libro.

presentazioni, testi).

blockchainworkshop.it

14

15

01

Capitolo primo

Cos’è una Blockchain?

La fiducia decentralizzata

FARE **Business** CON LA **Blockchain**

Capitolo primo

Cos’è una Blockchain?

La fiducia decentralizzata

La Blockchain è un registro di transazioni digitali con tre

caratteristiche fondamentali:

immutabile: a prova di manomissione (nul a viene

decentralizzato: senza un'autorità centrale (senza

modificato se pubblicato).

una banca o un governo).

18

La Blockchain consente ad una comunità di utenti di

registrare le transazioni in un registro condiviso all'interno

di tale comunità, in modo che, durante il normale

funzionamento, nessuna transazione

possa essere

modificata una volta pubblicata. C'è grande interesse

sul 'argomento Blockchain, ma pochissime persone la

comprendono. Non è magia, e non può risolvere tutti i

problemi. Come per tutte le nuove tecnologie, c'è la tendenza

a volerle applicare ad ogni settore per tentare di rendere

più innovativo un progetto dal punto di vista del marketing.

Questo capitolo ha lo scopo di rivelare il segreto di tale

distribuito: senza un server centrale ma su tanti

magia e spiegare in dettaglio come funziona la tecnologia

server ridondanti.

Blockchain. Arthur C. Clarke diceva che

“Ogni tecnologia sufficientemente avanzata è

indistinguibile dalla magia” [1].

1 Clarke, A. (1962), Profiles of the

Future, Harper & Row.

19

Blockchain 1.0: Bitcoin

La Blockchain di Bitcoin è memorizzata, mantenuta e

gestita in modo col aborativo da un gruppo distribuito

Nel 2008, all'apice della crisi di fiducia nel mondo di partecipanti. Questo, insieme ad alcuni meccanismi

finanziario, l'enigmatico Satoshi Nakamoto propone di criptografici, rende la Blockchain di Bitcoin resistente

ai

combinare diverse tecnologie e concetti informatici al tentativi di alterare il registro in un secondo momento

fine di creare una Criptovaluta chiamata Bitcoin: una (modificando i blocchi o falsificando le transazioni).

valuta elettronica in cui le transazioni fra gli utenti

vengono rese sicure da meccanismi criptografici invece Bitcoin è una Criptovaluta governata da un gruppo di

che da un'autorità centrale.

sviluppatori (Bitcoin Core developers) che incarnano la

filosofia descritta da Satoshi e la difendono da qualsiasi

Al ’interno del a Blockchain di Bitcoin, le informazioni che tentativo di cambiamento.

rappresentano il contante elettronico sono col egate ad un

indirizzo digitale associato ad una chiave. Gli utenti Bitcoin

possono firmare digitalmente con quel a chiave trasferendo

una quantità specifica di valuta elettronica ad un altro utente

e la Blockchain di Bitcoin registra pubblicamente questo

trasferimento, consentendo a tutti i partecipanti del a rete di

verificare in modo indipendente la validità del e transazioni.

Bitcoin

20

Blockchain 2.0: Ethereum

Nel 2013 il diciannovenne Vitalik

Buterin propone

una Blockchain totalmente programmabile chiamata

Ethereum che permette agli sviluppatori di costruire

applicazioni immutabili, decentralizzate e distribuite.

Queste applicazioni rendono possibile lo scambio di

qualsiasi valore (non solo Criptovaluta): contenuti digitali,

titoli di proprietà, azioni e qualsiasi cosa che vale e che,

per continuare ad avere valore, non deve essere duplicata,

proprio come il denaro contante. Ethereum è stato accolto

con grande entusiasmo dagli sviluppatori di software di tutto

il mondo che hanno iniziato a costruire insieme la visione che

Buterin ha delineato. Ethereum è in assoluto la più grande ed

inclusiva comunità di Blockchain al mondo.

La comunità di Ethereum raccoglie le

maggiori menti

provenienti da ogni settore, ceto sociale, genere e da

ogni parte del mondo. Ethereum viene creato e gestito da

persone unite dall'idea che la tecnologia della Blockchain

può cambiare il mondo attraverso l'uso di meccanismi

economici basati sulla teoria dei giochi chiamata

criptoeconomia.

Smart Contract

Le funzioni di base che i programmi su Ethereum svolgono

vengono chiamati Smart Contract.

I “contratti intel igenti” sono accordi digitali che vengono

eseguiti automaticamente sul a base di dati del mondo reale.

Un modo semplice di pensare a questi contratti è un “If-then

statement”. Se la condizione A esiste, al ora eseguono la

funzione B.

Diciamo ad esempio che Alice è una cantante famosa

e scrive una canzone assieme a Bob. Bob vuole essere

sicuro di venire compensato con la percentuale dei diritti

d’autore che gli spettano. Alice potrebbe attivare uno

Smart Contract su Ethereum in modo che ogni volta che

Spotify invia un pagamento di royalty sul suo conto, perché

qualcuno ascolta la loro canzone, la funzione smart girerà

automaticante il 50% dell'importo ricevuto sul conto di

Bob.

22

Gli Smart Contract hanno applicazioni che vanno oltre la *mostra che il volo è in ritardo di oltre due ore, il contratto*

musica.

intelligente viene attivato e l'assicurato viene pagato

automaticamente attraverso la Blockchain. Senza Smart

Un altro esempio di uno Smart Contract su Ethereum: Contract, l'assicurato dovrebbe presentare una richiesta

compro un'automobile e trasferisco il certificato di di risarcimento e attendere che qualche dipendente

proprietà ad uno Smart Contract che liquida per mio conto dell'ufficio sinistri della compagnia di

assicurazione lo

il fornitore. Ogni primo giorno del mese, per 36 mesi, io elabori, il che potrebbe richiedere da una a due settimane.

devo pagare un'importo della rata più gli interessi. Alla fine

dei 36 mesi lo Smart Contract mi trasferisce il certificato di Con lo Smart Contract, né la compagnia di assicurazione

proprietà dell'auto. Abbiamo creato una sorta di leasing né l'assicurato devono fare nul a. Questo crea fiducia

tra le

senza una società di leasing.

due parti anche perché non ci sono zone d'ombra - il cliente

può analizzare lo Smart Contract prima del 'acquisto del a

I processi che attualmente comportano interazioni manuali polizza sentendosi a proprio agio nel ricevere il risarcimento

tra due parti, possono ora essere automatizzati e il valore in caso di ritardo.

può essere spostato in tempo reale

attraverso la Blockchain

piuttosto che regolarsi giorni dopo come avviene con gli

istituti finanziari tradizionali.

Ethereum e gli Smart Contract sono qualcosa di straordinario

perché hanno la capacità di far decol are quel a che è stata

definita la “smart economy”, in cui processi manuali, lenti,

inclini al ’errore umano e al a frode, vengono sostituiti da

processi automatici completamente trasparenti e affidabili.

AXA offre un prodotto assicurativo per il trasporto aereo

che paga un assicurato in caso di ritardo del volo di due

o più ore. Si tratta di un sistema automatico che paga i

sinistri assicurativi utilizzando un semplice Smart Contract

su Ethereum: se il volo è in ritardo di oltre due ore, allora

l'assicurato viene risarcito. Lo Smart

Contract è collegato

FIZZY

a un database che monitora i tempi di volo. Se il database 23

Ethereum e ETH

Ethereum è una piattaforma per sviluppare e pubblicare

applicazioni su Blockchain utilizzando contratti intel igenti.

Per far funzionare questi Smart Contrats è necessario

comprare la Criptovaluta di Ethereum

chiamata **Ether** o

ETH. Si tratta di un' operazione semplicissima: basta andare

su un' App chiamata **COINBASE** che agisce da cambiavalute

(exchange) e comprare un po' di ETH in cambio di EUR.

L'Ether funziona più come una benzina digitale che come

una valuta digitale: nello stesso modo in cui una persona

deve rifornire l'auto con la benzina per viaggiare, per

eseguire le applicazioni su Ethereum serve l'ETH.

Nel precedente esempio di Alice e di Bob, Alice deve

acquistare una piccola quantità di ETH per alimentare il

suo Smart Contract che manda a Bob i soldi delle royalty.

La Blockchain di Ethereum funziona al o stesso modo del a

Blockchain di Bitcoin: una rete di computer esegue un

software che convalida le transazioni

attraverso il consenso

del a maggioranza. Le persone che gestiscono questi

computer sono chiamati **Miners** (minatori): i minatori di

Bitcoin sono compensati per le loro risorse con il pagamento

in Bitcoin mentre i minatori di Ethereum sono ricompensati

COINBASE

in Ether.

Il costo della transazione di Alice su Ethereum per pagare

le royalty di Bob, andrà al minatore che aggiunge alla

Blockchain il blocco contenente la transazione. Il minatore

riceverà inoltre nuovo Ether creato durante questa

transazione. Il model o economico di domanda e di offerta

che si applica a materie prime come il petrolio e il gas si

applica anche su Ethereum. Il petrolio è

prezioso perché

alimenta molte del e cose che usiamo nel a nostra vita

quotidiana - riscalda le nostre case e fa muovere le nostre

auto. Più saranno le persone e le imprese che svilupperanno

applicazioni basate su Ethereum, più alta sarà la domanda

di Ether e questo ne aumenterà il valore. Come per tutte

le Criptovalute, c'è una costante speculazione sul prezzo

basata sul ’ipotesi che la domanda di Ether aumenterà in

futuro. Poiché l’ETH è prezioso, scambiabile e trasferibile, la

comunità mondiale ha iniziato ad accettarlo come valuta.

dApp - Applicazioni decentralizzate

Le applicazioni che eseguono gli Smart Contract sul a

Blockchain di Ethereum sono chiamate “**dApp**”, o

applicazioni decentralizzate. Al o stesso modo in cui ogni

sviluppatore può creare un' app mobile sul sistema operativo

iOS di Apple per iPhone e iPad, gli sviluppatori di Ethereum

possono costruire software su l'infrastruttura Blockchain di

Ethereum.

L'utente finale di una dApp potrebbe non accorgersi della

differenza rispetto ad una normale app.

Ciò che la rende estremamente diversa è la tecnologia Questo Smart Contract potrebbe paradossalmente sostituire

sottostante, poiché le dApp funzionano sul a parte superiore un'azienda di gestione dei diritti tipo la SIAE e qualsiasi

del a Blockchain e possono essere utilizzate per trasferire musicista lo potrebbe utilizzare senza dover imparare un

il valore da una persona ad un'altra (Peer-to-Peer) senza nuovo linguaggio chiamato **Solidity** per scrivere uno Smart

intermediari.

Contract.

Qualcuno potrebbe utilizzare il codice dello Smart

Contract di Alice e aggiungere un altro Smart Contract che

scrive automaticamente: “5000 persone hanno ascoltato

la tua canzone in Italia”, inserendo delle funzionalità di

reportistica senza dover ogni volta riscrivere il codice.

L’esecuzione del e dApp sul a Blockchain offre anche grandi

vantaggi in termini di sicurezza: poiché le transazioni sono

distribuite e criptate in tutta la Blockchain di Ethereum. Non

esiste fisicamente un server dove un hacker potrebbe entrare

e ottenere l’accesso a tutti i dati di pagamento del e royalty.

In questo momento l’intera comunità di Ethereum,

Per tornare all’esempio di Alice ,

potrebbe esserci una dApp **composta da migliaia di singoli sviluppatori, startup**

***generica chiamata MusicRoyalty.sol che chiunque può* e aziende multinazionali, sta lavorando a una serie**

***utilizzare su Ethereum e che permette di programmare i* incredibile di progetti innovativi estremamente più**

***pagamenti percentuali per qualsiasi royalty e per qualsiasi* complessi del mio esempio di dApp MusicRoyalty.sol.**

gruppo di musicisti.

26

27

Token

Molti progetti su Ethereum hanno la propria Criptovaluta o

“Token”.

Compreso il concetto che Ethereum è una Blockchain che

permette di sviluppare applicazioni decentralizzate, le Per poter interagire con le loro dApp, i clienti devono

quali richiedono l'uso di una moneta chiamata ETH per acquistare il token nativo del a dApp. Ecco un'utile analogia:

farle eseguire, introduciamo un altro concetto abbastanza

destabilizzante:

quando si va a sciare si paga lo SkiPass e in cambio, si

ottiene una schedina o un braccialetto, che permette di

chiunque su Ethereum può creare la propria moneta.

salire sullo Skilift e fare slalom nelle piste. Con alcune

dApp, il token è il braccialetto e l'utente deve acquistarlo

per interagire con qualsiasi cosa offra la dApp.

28

Prendiamo ad esempio un progetto chiamato **LivePeer**.

LivePeer permette di affittare la propria potenza di calcolo in

eccesso al e persone che hanno bisogno di trasmettere video

in diretta senza censure. Se sono un video reporter, posso

acquistare **Token Livepeer** che mi permettono di utilizzare la

rete Livepeer per pubblicare il mio video in diretta, poi pago

le persone che mi affittano i loro computer con il Livepeer

token.

Il **Token Livepeer** è uno speciale **Smart Contract** e questa

transazione di pagamento è registrata sul a **Blockchain**

di Ethereum. Poiché i gettoni Livepeer sono anche una

Criptovaluta, possono essere scambiati sul libero mercato.

Se sono uno speculatore che non ha intenzione di usare

la rete Livepeer per affittare potenza di calcolo, posso

comunque comprare il gettone Livepeer in un exchange

nella speranza che si apprezzi in valore.

Come per **Bitcoin**, c'è un'offerta fissa di

Token Livepeer

quindi se la domanda del servizio aumenta, è ipotizzabile

che aumenti anche il valore del suo token.

Tokens

29

Blockchain 3.0 networks di Blockchain

Le implementazioni di Blockchain sono spesso pensate con uno scopo o una funzione specifica. C'è stato negli ultimi

anni un flusso costante di sviluppi nel campo della tecnologia a Blockchain e il settore è in continua evoluzione.

La tecnologia Blockchain può essere applicata al trasferimento di Criptovaluta come nel caso di Bitcoin e nel trasferimento

di qualsiasi valore, come anche nell'esecuzione di Smart Contract su Ethereum. Inoltre si può trasferire valore da una

Blockchain all'altra creando un network di network proprio come internet è una rete di reti.

In particolare, **Cosmos.network** fondato da **Jae Kwon** aspetti fondamentali. Ad esempio, cosa succede quando e **Ethan Buchman** e **Polkadot.network** fondato da **Gavin** un'organizzazione implementa una rete Blockchain e poi

Wood e **Robert Habermeier** ***sono due principali progetti*** decide di apportare modifiche ai dati memorizzati? Quando

che permettono di trasferire valore da una Blockchain si utilizza un database, la modifica dei dati effettivi può

all'altra.

essere effettuata attraverso una query e un aggiornamento

del database. Le aziende devono capire che, mentre le

Le aziende che stanno considerando l'implementazione modifiche ai dati effettivi del a Blockchain possono essere

del a tecnologia Blockchain devono comprenderne gli molto difficili, le applicazioni che utilizzano la Blockchain

come strato di dati lavorano intorno a

questo, trattando i Questo si chiama "**raggiungere il consenso**"e ci sono molti

blocchi e le transazioni successive come aggiornamenti o model i per farlo, ognuno con aspetti positivi e negativi

modifiche ai blocchi e al e transazioni precedenti.

per casi aziendali particolari. È importante capire che una

Blockchain è solo una parte di una soluzione.

Questa astrazione del software consente di modificare i

dati, fornendo al contempo una storia completa.

Ci sono due categorie generali di approcci al a Blockchain che

sono stati identificati: **Pubbliche** , ovvero senza permessi

Un altro aspetto critico del a tecnologia Blockchain è il modo (permissionless), e **Private** o **Federate** (permissioned).

in cui i partecipanti concordano sul fatto che una transazione

sia valida.

Pubbliche

Private

Federate

31

In una rete Blockchain pubblica chiunque può leggere del a Blockchain) contiene un col egamento criptografico

e scrivere alla Blockchain senza autorizzazione. Le reti al ’intestazione del blocco precedente.

Blockchain Private limitano la partecipazione a persone o

organizzazioni specifiche e

permettono controlli a grana Ogni transazione coinvolge uno o più utenti del a rete

più fine.

Blockchain e una registrazione di ciò che è successo, ed è

firmata digitalmente dal ’utente che ha inviato la transazione.

Conoscere le differenze tra queste categorie permette

ad un’organizzazione di capire quale sottoinsieme di

tecnologie Blockchain può essere

applicabile alle proprie

esigenze.

Malgrado la loro molteplicità e lo sviluppo rapido di nuove

tecnologie ad esse relative, la maggior parte delle reti di

Blockchain utilizzano dei concetti di base comuni.

Le Blockchain sono un registro distribuito composto da

blocchi.

Ogni blocco è composto da

un’intestazione contenente

metadati sul blocco e dati di blocco riferiti a un insieme di

transazioni e altri dati correlati.

Ogni intestazione di blocco (ad eccezione del primo blocco

La tecnologia Blockchain prende concetti esistenti e L’uso di tecnologia Blockchain non è una panacea e ci sono

collaudati e li fonde in un’unica soluzione.

implicazioni che devono essere considerate, ad esempio

come trattare con gli utenti malevoli, come applicare i

Questo libro esplora i fondamenti di come funzionano comandi e le limitazioni del e esecuzioni.

queste tecnologie e le differenze tra gli approcci alle

Blockchain, incluso il modo in cui i partecipanti alla rete Oltre al e implicazioni tecnologiche, ci sono implicazioni

concordano sulla validità di una

transazione e cosa succede operative e di control o che interessano il comportamento

quando è necessario apportare modifiche a una Blockchain del a rete. Ad esempio, nel e reti Blockchain Private o

esistente.

Federate, descritte più avanti in questo documento, ci sono

problemi di progettazione che determinano quale entità o

Inoltre, si esamina quando è il caso di utilizzare una quali entità opereranno e

governeranno la rete per la base

Blockchain.

utenti prevista.

33

La storia della Blockchain

2011

Sviluppo delle cryptovalute

2007

e delle loro applicazioni nelle

2015-2016

2017-2018

Satoshi Nakamoto

transazioni di denaro.

comincia a lavorare

2013

sui concetti di Bitcoin

Bitcoin raggiunge parità di

Evoluzione del mercato,

Viene progettato

e Blockchain.

valore con il dollaro (US).

esplorazione delle possibilità

Il primo sportello bancomat

2009

e nasce **Commerc.io**

dell'implementazione

di Bitcoin viene installato

Prima transazione

delle cryptovalute nelle

a San Diego.

Bitcoin nel block #170.

aziende.

2008

2010

2012

2014

2019

Bitcoin.org viene

Prima transazione nel

registrato.

mondo reale di

Implementazione nel mercato

Il block 181919 è

Nuove normative europee

10.000 BTC per

finanziario della

il più attivo con

sulla blockchain

Viene pubblicato il

il pagamento di

blockchain.

1.322 transazioni.

e legge italiana

primo documento legale

una pizza.

Paypal annuncia

sulla fatturazione elettonica.

Coinbase, un bitcoin

sulla Bitcoin.

l’integrazione di Bitcoin.

wallet, viene fondato

a San Francisco.

Evoluzione degli

smart contracts.

Le idee fondamentali al a base del a tecnologia Blockchain Il documento descrive un model o di consenso per

sono emerse tra la fine degli anni ‘80 e l’inizio degli anni ’90.

raggiungere un accordo su un risultato in una rete di

computer in cui i computer o la rete stessa possono essere

Nel 1989, **Leslie Lamport** ha sviluppato il protocol o Paxos inaffidabili.

e nel 1990 ha presentato l'articolo The Part-Time Parliament

al periodico ACM Transactions on Computer Systems; Nel 1991, una catena di informazioni firmate è stata utilizzata

pubblicato poi in un numero del 1998 [2].

come libro mastro elettronico per la firma digitale dei

documenti, in modo tale da poter facilmente mostrare che

nessuno dei documenti firmati nel a col ezione era stato

2 Lamport, L. (1998), The Part-Time Parliament in “ACM Transactions on

modificato.

Computer Systems”, 16, 2 (May 1998), 133-169.

34

Questi concetti sono stati combinati e applicati al contante di organizzarsi. Utilizzando una gestione del a Blockchain

elettronico nel 2008 e descritti nel documento **“Bitcoin: A** basata sul consenso è stato creato un meccanismo di

Peer-to-Peer Electronic Cash System” , che è stato pubblicato autocontrol o che assicurava che solo le transazioni e i

con lo pseudonimo di **Satoshi Nakamoto**, e poi più tardi nel blocchi validi fossero aggiunti al a Blockchain.

2009 con la creazione del a Bitcoin cryptocurrency Blockchain

network. La ricerca di Nakamoto conteneva il progetto che la In Bitcoin la Blockchain permetteva agli utenti di essere

maggior parte dei moderni schemi di criptografia valutaria pseudo-anonimi.

Ciò significa che gli utenti sono anonimi,

seguono (anche se con variazioni e modifiche). Bitcoin è stata ma i loro identificatori di conto (indirizzi) non lo sono. Inoltre,

solo la prima di molte applicazioni del a Blockchain.

tutte le transazioni sono pubblicamente visibili. Questo ha

permesso a Bitcoin di offrire uno pseudo-anonimato, poiché

Le monete elettroniche esistevano prima di Bitcoin (ad gli account possono essere creati senza alcun processo

esempio, Ecash e NetCash), ma nessuna di esse ha raggiunto di identificazione o autorizzazione, processi tipicamente

una diffusione utile. L’uso del a Blockchain ha permesso di richiesti dal e leggi anti-riciclaggio Anti Money Laundering

implementare Bitcoin in modo distribuito, così che nessun (AML) e Know-Your-Customer (KYC).

singolo utente potesse control are il registro elettronico e

non esistesse un singolo punto di rottura promuovendone

l’uso.

Il suo vantaggio principale è stato quello di consentire

transazioni dirette tra utenti senza la necessità di una

terza parte fiduciaria.

Ha inoltre consentito l’emissione di nuova criptovaluta

in modo predefinito agli utenti che riescono a pubblicare

nuovi blocchi e a mantenere copie del registro, i minatori.

Il pagamento automatico ai minatori ha permesso

un'amministrazione distribuita del sistema senza la necessità

35

Le tre caratteristiche chiave della tecnologia Blockchain

Poiché Bitcoin era pseudo-anonimo, era essenziale disporre di meccanismi per creare fiducia in un ambiente in cui gli utenti

non potevano essere facilmente identificati. Prima del 'uso del a tecnologia Blockchain, questa fiducia

era in genere fornita

attraverso intermediari fidati da entrambe le parti. Senza intermediari fidati, la fiducia necessaria al ’interno di una rete

Blockchain è resa possibile da tre caratteristiche chiave del a tecnologia Blockchain, descritte di seguito.

• **Immutabile:** la tecnologia del a • **Decentralizzato:** il registro del a • **Distribuito:** la Blockchain può

Blockchain utilizza una scrittura

Blockchain è condiviso tra più

essere distribuita: questo permette

nel libro mastro per fornire una

partecipanti. Ciò garantisce la

di scalare il numero di nodi di

storia completa del e transazioni.

trasparenza tra i partecipanti ai

una rete Blockchain per renderla

A

differenza

dei

database

nodi del a rete Blockchain.

più resistente agli attacchi di

tradizionali, le transazioni e i

malintenzionati. Aumentando il

valori in una Blockchain non

numero di nodi, la capacità di un

possono essere sovrascritti e

malintenzionato di influenzare il

sono criptograficamente sicuri,

protocol o di consenso utilizzato

garantendo che i dati contenuti nel

dal a Blockchain è ridotta.

registro non siano stati manomessi

e siano attestabili.

Quando le persone hanno cominciato a capire il funzionamento

della Blockchain, hanno iniziato ad usarla per altri scopi, fra cui:

- **Scambio di beni digitale di valore**

- **Identità**
- **Accordi**
- **Diritti di proprietà**

37

Ethereum è ad oggi l'innovazione a Blockchain più completa

dopo Bitcoin. Come le implementazioni di cloud computing,

sono emersi diversi tipi o categorie di Blockchain.

Analogamente al cloud, si hanno Blockchain pubbliche

alle quali tutti possono accedere, Blockchain Private per

gruppi limitati all'interno di un'organizzazione e consorzi

di Blockchain che vengono utilizzati in collaborazione con

altri.

Blockchain Pubbliche

Una Blockchain Pubblica come Bitcoin, Ethereum, Zcash o Nel a Blockchain Pubblica, poiché nessun utente è

Monero è quel a che i creatori iniziali hanno immaginato come implicitamente

affidabile per verificare le transazioni, tutti

una Blockchain a cui tutti possono accedere, una Blockchain gli utenti seguono un algoritmo che verifica le transazioni

in cui le transazioni sono incluse, se e solo se, sono valide e in impegnando risorse software e hardware per risolvere

cui tutti possono contribuire al processo di consenso. Come un problema con la forza bruta (cioè, risolvendo il puzzle

anticipato, il processo di consenso determina quali blocchi criptografico).

Il minatore che arriva per primo al a

vengono aggiunti al a catena e quale è lo stato attuale. soluzione viene premiato, e ogni nuova soluzione, insieme

Invece di usare un server centrale, la Blockchain Pubblica al e transazioni che sono state utilizzate per verificarla,

è assicurata da una verifica criptografica supportata da costituisce la base per il prossimo problema da risolvere. I

incentivi per i minatori, e chiunque può essere un minatore concetti utilizzati per la verifica sono la **Proof of Work (PoW)**

per aggregare e pubblicare queste transazioni.

che utilizza molta energia elettrica o
Proof of Stake (PoS)

che non fa uso di energia ma dei Token stessi.

38

Blockchain Federate

Una Blockchain Federata come Commercio.network è un libro ottenere prove criptografiche di alcune parti del o stato del a

mastro distribuito in cui il processo di

consenso è control ato Blockchain. Questo tipo di Blockchain federate sono libri

da un insieme preselezionato di nodi con le caratteristiche mastro distribuiti che possono essere considerate “ibride”.

specifiche di un consorzio di aziende.

Commercio.network è una rete aperta a 250 milioni di aziende

ognuna del e quali, può gestire un suo nodo e 100+ aziende

possono gestire un nodo validatore e devono firmare ogni

blocco, affinché sia valido. Il diritto di leggere la Blockchain

può essere pubblico o limitato ai partecipanti.

Ci sono anche percorsi ibridi insieme ad un API che permette ai

membri del pubblico di fare un numero limitato di richieste e

Blockchain Private

Una Blockchain completamente privata come quel e Le Blockchain Private potrebbero fornire soluzioni ai problemi

sviluppate con Hyperledger e R3 Corda è una Blockchain in del e imprese finanziarie, compresi gli agenti di conformità

cui i permessi di scrittura risultano centralizzati in un'unica per regolamenti, l'antiriciclaggio (AML) e le leggi KYC (Know-

organizzazione, mentre i permessi di lettura possono Your-Customer).

essere pubblici o limitati in misura arbitraria. Le probabili

applicazioni includono la gestione del database e l'auditing

interno ad una singola azienda, per cui la leggibilità pubblica

in molti casi può non essere necessaria, anche se in altri è

auspicabile una revisione pubblica.

Confronto fra le Blockchain

ATTENZIONE!

Nel caso del e reti Blockchain pubbliche che permettono **Se un utente perde la chiave, qualsiasi risorsa associata**

a chiunque di creare degli account e

partecipare in modo **a quella chiave viene IRRIMEDIABILMENTE persa, perché**

anonimo, le tre caratteristiche del a Blockchain evidenziate

non è possibile rigenerare la stessa chiave.

precedentemente, offrono un livel o di fiducia tale, da

consentire agli individui e al e organizzazioni di operare

direttamente senza alcuna conoscenza l’uno del ’altro.

La possibilità di accedere ad una Blockchain senza dover

chiedere il premesso a qualcuno è forse la caratteristica più

innovativa e dirompente rispetto al passato.

Dal punto di vista filosofico si può dire che per la prima volta

nell'umanità una persona o un'azienda sono realmente

libere di disporre delle proprie informazioni senza doversi Con riferimento invece al e reti Blockchain Private o

affidare ad un terzo ente fiduciario.

Federate, dove esiste un control o del ’accesso più elevato e

deve essere presente una certa fiducia tra gli utenti, queste

quattro caratteristiche aiutano a rafforzare tale fiducia.

La distinzione tra Blockchain Pubbliche, Federate e Private

è importante. Anche per chi vuole adottare i DLT “vecchia

scuola”, cioè i Distributed Ledger Technology che preferiscono

un sistema tradizionale centralizzato, i DTL mantengono la

verificabilità criptografica.

Rispetto al e Blockchain Pubbliche, le Blockchain Private

hanno una serie di vantaggi, ad esempio l'operatore privato

del a Blockchain può cambiare le regole di una Blockchain

quando vuole. Quindi se si tratta di una Blockchain tra differenza di latenza non scomparirà mai perché purtroppo,

partner finanziari, qualora si scoprano bug nel codice del la velocità del a luce non aumenta di due volte ogni due anni

protocol o, sarà in grado di modificare le transazioni. Al o come fanno i processori secondo la legge di Moore. Inoltre

stesso modo, potranno cambiare gli equilibri e generalmente se i permessi di lettura sono limitati, le Blockchain Private e

fare qualsiasi cosa voglia.

Federate possono fornire un maggiore livel o di privacy.

Talvolta questa funzionalità è necessaria, come nel caso ***Alla luce di tutto questo, potrebbe sembrare che le***

del registro di proprietà se viene rilasciata una transazione ***Blockchain Private possano rappresentare una scelta***

sbagliata, o quando qualche hacker ha ottenuto l'accesso ***migliore per le aziende. Tuttavia, il valore più alto è nelle***

ed è diventato il nuovo proprietario. Questo vale anche per ***Blockchain Pubbliche e Federate in virtù dei principi***

una Blockchain Pubblica se il governo ha chiavi di accesso ***filosofici scritti nel protocollo:***

(backdoor). Sul e Blockchain Private e Federate le transazioni

Libertà, Neutralità e Apertura.

sono meno costose, poiché devono essere verificate solo

da pochi nodi che possono essere considerati affidabili e **I vantaggi delle Blockchain Pubbliche e Federate**

hanno una potenza di calcolo molto elevata. Le Blockchain **rientrano in due grandi categorie:**

Pubbliche tendono ad avere costi di transazione più elevati,

ma questo cambierà man mano che si avrà la scalabilità • ***le Blockchain Pubbliche e Federate forniscono un modo***

necessaria, fra qualche anno tali costi si abbasseranno.

per proteggere gli utenti finali dagli sviluppatori,

stabilendo che ci sono alcune cose che anche gli

I miglioramenti nel a tecnologia del a Blockchain Pubblica,

sviluppatori di un'applicazione non possono fare.

come la Proof of Stake di Tendermint, previsti per i

prossimi anni, potranno avvicinare le Blockchain Pubbliche • ***le Blockchain Pubbliche e Federate sono aperte, e***

al 'ideale di "conferma istantanea". Le Blockchain Private

quindi utilizzate da molte entità. Questo fornisce alcuni

e Federate,d'altra parte, saranno sempre più veloci e, la

effetti di rete. Se abbiamo sistemi di trasferimento

di valore su una Blockchain, o una Criptovaluta sulla

stessa Blockchain, allora possiamo ridurre i costi di

trasferimento quasi a zero con uno Smart Contract.

Essere Liberi

42

43

Termini più comuni utilizzati

La terminologia per la tecnologia Blockchain varia molto da un'implementazione al 'altra.

In questo documento ci riferiremo a:

• **Blockchain:** il vero e

• **Blockchain technology: • Rete Blockchain:** la rete

• **Implementazione di**

proprio libro mastro.

un termine per

in cui viene utilizzata una

una Blockchain: una

descrivere la tecnologia

Blockchain.

Blockchain specifica

nel a forma più generica.

(Bitcoin, Ethereum e

Commercio.network).

New!

- **Utente della**

• **Node:** un sistema

• **Validator Node:**

• **Full Node:** un nodo • **Light Node:** un

Blockchain:

individuale

un nodo che

che memorizza

nodo che non

una persona,

al ’interno di una

memorizza l’intera

o mantiene

memorizza o

organizzazione,

rete Blockchain .

Blockchain, e

una copia del a

mantiene una

entità, azienda,

si occupa di

Blockchain e

copia del a

governo, ecc. che

assicurarsi che le

può propporre

Blockchain ma

utilizza una rete

transazioni siano

di scrivere una

deve mandare

Blockchain.

valide .

transazione.

le transazioni ad

un ful node per

poterle scrivere.

45

02

Capitolo secondo

Cosa può fare un’azienda con la

Blockchain?

L’azienda e il web 3.0

FARE **Business** CON LA **Blockchain**

Capitolo secondo

Cosa può fare un’azienda con la Blockchain?

L’azienda e il web 3.0

Le esigenze aziendali

Le imprese hanno esigenze molto diverse da quel e dei singoli utenti su una rete Peer-to-Peer: esse devono gestire

i dati sensibili in grandi volumi, monitorare la qualità e rispondere agli standard di sicurezza e normativi dei loro

settori industriali, sia che si tratti del ’emissione di ID, del ’esecuzione di operazioni commerciali, del a tracciabilità

dei container o del ’etichettatura dei prodotti farmaceutici. Sicurezza, certezza e responsabilità su scala sono

fondamentali per un’azienda ad alte prestazioni.

Le esigenze del e imprese si suddividono in quattro categorie:

Autorizzazione

Privacy

Prestazioni

Finalità

48

Autorizzazione: i casi d’uso **Privacy:** i dati al ’interno

Prestazioni: le imprese

Finalità: le istituzioni

aziendali spesso richiedono

di transazioni specifiche

devono avere l'infrastruttura che trasferiscono grandi

che solo le parti autorizzate

(nome del prodotto,

per elaborare migliaia di

quantità di denaro hanno

possano unirsi al a rete e che quantità, prezzo, indirizzo,

transazioni al secondo e

bisogno di certezza circa

i partecipanti abbiano ruoli

informazioni finanziarie

tol erare picchi periodici

l’esito del e transazioni.

diversi in lettura, accesso e

personalmente identificabili, nel ’attività di rete.

I fondi devono essere buoni

scrittura.

ecc.), dovrebbero essere

Un ordine di vendita con

e i pagamenti devono essere

trattenuti o resi disponibili

mil e righe, ad esempio,

definitivi.

ai partecipanti al a rete a

innesca una cascata di

seconda del loro ruolo. Uno

eventi transazionali.

spedizioniere, ad esempio,

Nel e economie di rete

potrebbe non avere bisogno di oggi, le imprese

di conoscere il contenuto di

devono essere in grado di

un determinato container,

raccogliere, convalidare

ma solo che il container è

e pubblicare un volume

arrivato. Anche le norme

sempre maggiore di

bancarie limitano l’accesso

transazioni diverse.

ai dati del e transazioni.

49

Le tre componenti della Blockchain

La Blockchain è una tecnologia abilitante che sta

cambiando il modo in cui pensiamo e realizziamo le

applicazioni business ma per capirla

occorre ripetere le

tre componenti che la rendono possibile: sebbene queste

esistano da tempo, non sono mai state utilizzate insieme **Il Software**, come descritto in dettaglio nel precedente capitolo,

all'interno di una tecnologia.

è un insieme di tre componenti: un database in sola scrittura, un

sistema in networking che col ega più computer fra di loro (Peer-

to-Peer) e un meccanismo di consenso

che permette di decidere

quali transazioni possono essere scritte e quali no.

50

La Criptoeconomia è l'insieme del e Criptovalute e del a Teoria **La Criptografia** è utilizzata in varie parti per fornire sicurezza a dei Giochi. Quest'ultima non ha a che fare con i giocattoli ma è una rete Blockchain e si fonda su tre concetti di base: hashing, chiavi lo studio di model i matematici di conflitto e cooperazione tra e firme digitali. Un "hash" è un'impronta digitale unica che aiuta a decisori razionali intel igenti. Resa famosa dal

film “A Beautiful verificare che una certa informazione non sia stata alterata, senza la Mind” che racconta la vita del premio Nobel per l’economia John necessità di vederla effettivamente. Le chiavi sono utilizzate coppia

Nash, è legata alla Blockchain nel a soluzione del famoso problema una pubblica e una privata. Per analogia, immaginate una porta che

dei Generali Bizantini, che mentono sul coordinamento del loro ha bisogno di due chiavi per essere aperta. In questo caso, la chiave attacco per garantire la vittoria all’avversario.
L’implementazione pubblica viene

utilizzata dal mittente per cifrare informazioni che di una “Byzantine Fault Tolerance” (BFT) è importante perché possono essere decifrate solo dal proprietario del a chiave privata.

parte dal presupposto che non ci si può fidare di nessuno. Ci sono Non si rivela mai la chiave privata a nessuno. Una firma digitale è un

implicazioni fondamentali per questo nuovo metodo finalizzato a calcolo matematico che viene utilizzato per dimostrare l’autenticità

raggiungere la sicurezza nel carattere definitivo di una transazione, di un messaggio o documento (digitale). La

criptografia si basa sul

perché mette in discussione l'esistenza e il ruolo degli attuali concetto di chiave pubblica/privata. Visibilità pubblica, ma control o intermediari di fiducia, che detengono l'autorità tradizionale sul a privato. È un po' come il tuo indirizzo aziendale: si può pubblicare

convalida del e transazioni. Perché abbiamo bisogno di un'autorità un sito web del 'azienda, ma questo non dà alcuna informazione su

centrale per garantire la fiducia, se possiamo ottenere la stessa come avvengono i vostri processi di produzione. Avrete bisogno del a

affidabilità attraverso una rete in cui la fiducia è incorporata in vostra chiave privata per entrare in azienda e, poiché avete dichiarato essa? La criptoeconomia attraverso la Criptovaluta è ciò che quel ’indirizzo come vostro, nessun altro può rivendicare un indirizzo rende sicura una Blockchain, non la tecnologia. Attraverso un simile. Sebbene i concetti di criptografia siano in circolazione da un po’

processo chiamato Mechanism Design, si possono creare degli di tempo, sul a Blockchain essi vengono combinati con l’innovazione

incentivi criptoeconomici che spingono

le persone a comportarsi del a Teoria dei Giochi, dove l'incertezza è limitata da una certezza

in modo corretto. Sul a Blockchain costa meno essere onesti che matematica. È possibile provare matematicamente che è stato fatto

essere disonesti.

qualcosa senza dover necessariamente mostrarlo agli altri.

Molto forte.

I 10 benefici della Blockchain:

1. Riduzione dei costi: diretti o indiretti.

2. Aumento della velocità: eliminazione dei ritardi.

3. Maggiore trasparenza: fornire le informazioni giuste al e persone giuste.

4. Maggiore privacy: proteggere i consumatori e le imprese con control i più granulari.

5. Riduzione dei rischi: minore esposizione al e frodi, minori manomissioni.

6. Maggiore accesso: accesso più equo e trasparente.

7. Aumento della produttività: più lavoro prodotto.

8. Aumento dell'efficienza: elaborazione o segnalazione più rapida.

9. Maggiore qualità: meno errori o maggiore soddisfazione.

10. Miglioramento dei risultati: profitti e crescita.

La diversità è la forza della

Blockchain

La sicurezza è il fattore più importante di una Blockchain perché deve rendere

difficile, a qualsiasi attore o evento, di controllare o danneggiare il 51% dei suoi

nodi. La diversità è la forza di una Blockchain:

Diversità di giurisdizione: i nodi del a Blockchain dovrebbero essere control ati

da diverse entità al ’interno di più

giurisdizioni, cosicché diventi quasi impossibile

utilizzare mezzi legali per fermare la rete.

Diversità geografica: i nodi del a Blockchain dovrebbero essere distribuiti in tutto

il mondo, in modo che diventi quasi impossibile per una catastrofe naturale, (come

un'al uvione o un terremoto) danneggiarli tanto da causare l'arresto del a rete.

Questa diversità geografica deve

rispettare la legislazione sul a privacy.

Diversità del cloud: l'infrastruttura cloud dei server dovrebbe essere composta da

diversi fornitori (ad esempio AWS, Azure, Google Cloud, DigitalOcean), in modo che

diventi quasi impossibile per un provider di hosting interrompere la rete.

Diversità del sistema operativo: i server di nodi del a Blockchain dovrebbero

funzionare su una pletora di sistemi operativi, quindi un exploit di 0day in un

sistema

operativo non può essere utilizzato per fermare la rete.

Diversità di linguaggio: i server di nodo del a Blockchain dovrebbero essere scritti

in diversi linguaggi di programmazione, quindi un bug in un nodo, non può essere

usato per fermare la rete.

54

55

Le 3 proprietà della Blockchain

Abbiamo compreso che la Blockchain è un sistema fiduciario reso possibile dal a tecnologia togliendo il fattore umano, che

è sempre l'anel o debole.

Questa fiducia necessaria al 'interno di una rete Blockchain, come è stato più volte ripetuto in questo libro, è resa possibile da

tre caratteristiche chiave intrinseche nel a tecnologia in questione:

- **Decentralizzazione**

- **Immutabilità**

• Distribuzione

Per ognuna di queste tre proprietà della Blockchain è possibile immaginare alcuni esempi di casi d'uso specifici.

Decentralizzazione

Il registro della Blockchain è condiviso tra più partecipanti.

Ciò garantisce la trasparenza tra i partecipanti ai nodi

della rete Blockchain senza che ci sia la necessità di avere

un' autorità centrale che la controlli.

Fiducia decentralizzata: tutte le Blockchain sono servizi di

fiducia, tale fiducia non si applica solo al e transazioni ma

si estende a dati, servizi, processi, identità, business logic,

termini di un accordo o oggetti fisici. Si applica a quasi tutto

ciò che può essere digitalizzato come bene (intel igente) con

un valore intrinseco o correlato ad esso.

Infrastruttura decentralizzata: la Blockchain può

anche essere vista come un approccio di progettazione di

software che lega insieme un certo numero di computer

che comunemente obbediscono al o stesso processo di

“consenso” per rilasciare o registrare le informazioni in loro

possesso, e dove tutte le relative interazioni sono verificate

dal a criptografia.

Database decentralizzato: la Blockchain distrugge il

paradigma degli attuali database proprietari. Una Blockchain

è come un luogo dove si memorizzano i dati semi-pubblici

in uno spazio. Chiunque può verificare che tu abbia messo

quel ’informazione, perché il contenitore ha la tua firma, ma

solo tu puoi sbloccare, in modo sicuro, ciò che c’è al ’interno

del contenitore, perché solo tu hai le

chiavi private di quei

dati.

57

Immutabilità

A differenza di un classico database, le transazioni e i valori

in una Blockchain non possono essere sovrascritti e sono resi

sicuri da sistemi criptografici che rendono evidente se i dati

sono stati manomessi

Piattaforma monetaria: la Criptovaluta è sicuramente

l'elemento più "visibile" in una Blockchain, soprattutto se essa

è pubblica come lo sono Bitcoin (BTC) o Ethereum (ETH). Ogni

trasferimento di moneta è immutabile e lo stesso Token non

può essere dato a due persone diverse contemporaneamente

(double spending). La Criptovaluta è un'unità di conto economica

per le operazioni e un sistema per

incentivare la sicurezza di una

Blockchain. A volte è rappresentata da un Token, che è un'altra

forma di un asset sottostante

Piattaforma di transazioni: una rete Blockchain può

convalidare una serie di transazioni relative al valore del a

Criptovaluta, di documenti o di beni che sono stati digitalizzati in

un Token. (tokenizzati). Ogni volta che si raggiunge un consenso

una transazione viene registrata in modo immutabile su un

“blocco”, che è uno spazio di archiviazione.

Piattaforma di verifica: la Blockchain tiene traccia di queste

transazioni che possono essere successivamente verificate

come avvenute. La Blockchain è quindi questa gigantesca

piattaforma di verifica del e transazioni in grado di gestire sia

micro-transazioni che le transazioni di

grande valore.

58

Distribuzione

Aumentando il numero di nodi del server, diminuisce la

capacità di un hacker o di un governo di bloccare la rete.

Diventa inarrestabile.

Registro distribuito: la Blockchain è anche un registro

distribuito, pubblico, con data e ora, che tiene traccia di

ogni transazione elaborata sul a sua rete, consentendo al

computer del ’utente di verificarne la validità in modo che

non ci possa mai essere un doppio conteggio. Questo registro

può essere condiviso tra più parti e può essere privato,

pubblico o semi-privato

Exchange distribuito: la Criptovaluta è al a base del a

Blockchain. Quando la Criptovaluta viene considerata

come una qualsiasi valuta, essa può diventare parte di uno

strumento finanziario, portando al o sviluppo di una varietà

di nuovi prodotti finanziari Fintech: **derivati / opzioni /**

swap / strumenti sintetici / investimenti / prestiti .

Inoltre molti altri strumenti tradizionali avranno la loro

versione digitale, creando così un nuovo mercato borsistico

di negoziazione dei servizi finanziari

decentralizzati.

Rete distribuita: dal punto di vista del ’architettura, lo

strato di base del a Blockchain è una rete Peer-to-Peer. La

rete è il computer e una Blockchain risulta distribuita perché

è composta da migliaia di nodi col egati. La rete è il computer.

In sostanza, una Blockchain non è un cloud ma è più come

una leggera nebbia che è veramente ovunque.

I 4 Fattori Critici per l'implementazione della Blockchain in una Organizzazione

Ci sono delle cose che si possono fare da soli. Altre è meglio farle insieme. La Blockchain è una di queste.

Le aziende di tutti i settori dovranno affrontare una complessa e potenzialmente controversa serie di domande.

Comprensione e Consapevolezza

Collaborazione e Federazione

Come posso aumentare la comprensione della Blockchain Quali problemi e quali opportunità condivide la mia

nella mia organizzazione?

organizzazione con le altre del suo settore?

I problemi principali che si associano alla Blockchain sono una La forza del a Blockchain sta nel creare massimo valore per le profonda incomprensione del e tecnologie ad essa associate e aziende che operano in un medesimo settore industriale e in aree

un diffusa mancanza di comprensione del suo funzionamento, con le stesse problematiche e le stesse opportunità. Ciò che però

soprattutto in settori diversi da quel o bancario.

risulta ancora problematico nei metodi di applicazione attuali è che

questi risultano approcci a compartimenti stagni. Le aziende infatti

si focalizzano sul e proprie Blockchain Private annul ando di fatto il

valore primario del a Blockchain, ovvero l'effetto rete, e producendo

così un risultato meno efficiente di un approccio tradizionale.

60

Cultura aziendale

Costi e Benefici

Chi sarà più colpito dall'implementazione di un progetto Quali sono i costi e benefici di un progetto Blockchain?

blockchain?

Anche se molti settori hanno già subito significative trasformazioni con la Le startup non si pongono questa domanda e

hanno già iniziato Digital Transformation, l'implementazione del a Blockchain rappresenta a utilizzare la tecnologia Blockchain creando nuove imprese e un ulteriore e totale al ontanamento dagli approcci tradizionali.

soluzioni che vadano a sostituire quel e esistenti. Sono invece le

Essa fonda la sua affidabilità e la sua autorità su una rete decentralizzata, imprese tradizionali a porsi questa domanda, perché i benefici non piuttosto che su un'istituzione centrale e questa perdita di control o può sono necessariamente evidenti. Per le grandi aziende, la Blockchain essere profondamente destabilizzante per le

aziende. Una Blockchain si è presentata inizialmente come qualcosa di non previsto e poco

è costituita per circa l'80% dal cambiamento dei processi aziendali e comprensibile. Nessuna azienda in questo momento però se la per il 20% dal 'implementazione del a tecnologia. Ciò significa che è sente di ignorare completamente la Blockchain perché, data la necessario un approccio più aperto per comprendere le opportunità e i sua graduale espansione, si teme che un giorno un'altra azienda

cambiamenti in avvenire.

concorrente, che si basa su un sistema

Blockchain, possa intaccare

il suo business.

61

Il valore della Blockchain per

un'azienda

Non tutti i progetti Blockchain devono necessariamente Una Blockchain Federata come Commercio.network nasce

essere disgreganti dello status quo per generare valore.

con il preciso scopo di aiutare le

aziende a sfruttare la

Blockchain in modo semplice e veloce, è ospitata su reti

Gli evidenti benefici derivanti dal a riduzione del a complessità ***informatiche di operatori certificati che offrono accesso***

e dei costi del e transazioni, nonché dal miglioramento del a ***controllato, scalabilità e un forte livello di privacy.***

trasparenza e dei control i, possono essere colti da qualsiasi

azienda nel mondo. Creare un sistema che permetta al e

aziende di scambiare documenti commerciali tradizionali

attraverso la Blockchain può generare abbastanza valore

per favorire un'adozione massiccia a più livel i. Gli incentivi

economici per cogliere le opportunità di valore stanno

spingendo le aziende a sfruttare la Blockchain piuttosto che

farsi sorpassare da altri che la usano. Pertanto, il model o

commerciale che ha maggiori

probabilità di successo a

breve termine è quel o federato. Una Blockchain Pubblica

come Bitcoin, non ha un'autorità centrale e rappresenta un

percorso di disintermediazione monetaria totale. Ethereum,

con la sua capacità di essere programmabile, è invece uno

strumento che si adatta perfettamente a chi lo utilizza per

qualsiasi scopo, ma in questo momento non ha la scalabilità

necessaria per gestire le necessità del e aziende.

62

Come implementare la Blockchain in

azienda in 5 fasi

Per implementare qualsiasi nuova tecnologia come la in tutte queste aree, ma esse possono col aborare con aziende

Blockchain è necessario seguire un percorso di acquisizione esterne per aspetti specifici di queste fasi. Un network di

del e competenze, per non fare passi falsi e non creare aziende italiane ha sviluppato un percorso formativo sul a

del e cattedrali nel deserto che imbarazzano l'azienda e Blockchain chiamato BlockchainWorkshop.it che permette di

ne sprecano le risorse. Abbiamo identificato cinque aree acquisire in tempi rapidi tutte le conoscenze necessarie.

di competenza divise in cinque fasi di implementazione La ***Conoscere i fondamenti della Blockchain è una competenza***

maggior parte del e aziende non può sviluppare competenze ***imprescindibile tanto importante quanto sviluppare delle***

applicazioni.

Blockchain Workshop

63

Fase 1 Educazione: imparare le caratteristiche di base del a

tecnologia Blockchain, che classi di problemi genericamente

può risolvere e le opportunità che la Blockchain offre

Fase 2 Problem/Solution Fit: identificazione del e aree di

problemi aziendali che la tecnologia attuale non risolve e

analisi del se e dove la Blockchain può essere la soluzione.

64

Fase 3 App Design: di quali soluzioni funzionali avremo

bisogno per affrontare il problema che abbiamo scoperto

nel a fase precedente? In che modo influenzerà ciò che

stiamo facendo, compresi i processi aziendali, i requisiti

contrattuali e legali?

Fase 5 Gestione di progetto: Manutenzione continua del

software, supporto, evoluzione iterativa, implementazioni di

nuove funzionalità e aggiornamenti.

Fase 4 Sviluppo software: scelta del a tecnologia, scelta dei

fornitori, integrazione e implementazione del a Blockchain in

azienda e audit di sicurezza.

65

Quale modello di Blockchain per la tua
Il valore del ’opzione a lungo termine di Commercio.

Azienda?

network è l’interoperabilità con la rete pubblica principale

di Ethereum, che offre portata globale, estrema resilienza

Creare una propria Blockchain Privata o Pubblica per ed elevata integrità. La compatibilità con la rete

principale,

un'azienda è un'impresa costosa. Essa comporta la messa ridurrà in modo significativo la quantità di investimenti

in campo di un team di sviluppatori specifici di Blockchain attuali del e aziende nel 'infrastruttura IT e nel a sicurezza.

e la spesa di mesi e diversi milioni di euro per scrivere il

codice personalizzato.

Commercio.network con il proprio consorzio internazionale

si pone a metà strada fra la Blockchain Pubblica e la

Nel 2018 dall'iniziativa di 25 imprenditori in Italia è nata Blockchain Privata, con una soluzione ibrida che prende il

una nuova Blockchain Federata specifica per le aziende. meglio dei due mondi. Su Commercio.network le aziende

Commercio.network LA BLOCKCHAINDEI DOCUMENT™, mantengono le transazioni private, ma lavoreranno insieme

aperta a 250 milioni di imprese, dove ogni azienda può per costruire infrastrutture IT condivise, sicure e a prova di

utilizzare un suo nodo e 42 aziende possono gestire un futuro, piuttosto che continuare a duplicare l'infrastruttura

nodo validatore che certifica le transizioni, firmando per i propri casi d'uso. L'infrastruttura condivisa Commercio.

ogni blocco.

network libererà l'innovazione e sbloccherà le risorse che

Commercio.network ha semplificato radicalmente la in precedenza erano congelate tra organizzazioni non

creazione e il funzionamento di Blockchain per le imprese. comunicanti.

Attualmente Commercio.network offre al e organizzazioni ***Il modo più semplice ed economico per implementare la***

aziendali l'accesso al a piattaforma per la registrazione e la ***tecnologia della Blockchain non è dunque quello di creare***

configurazione di un ambiente in pochi minuti.

una Blockchain da zero ma di unirsi ad una Blockchain

esistente.

Commercio.network

66

Commercio.network è stata progettata per essere un sistema:

- **Economico**
- **Aperto**
- **Flessibile**
- **Adatto alla cooperazione tra più**

aziende

67

In termini di coordinamento dei dati, Commercio.network

funziona come un libro mastro distribuito, ma la sua

architettura ha anche livelli unici che rafforzano e creano

nuove possibilità per i sistemi aziendali. Per coloro che

vogliono comprendere a fondo le diverse funzionalità, sul

sito Commercio.network è presente una guida dettagliata

di tutti i moduli disponibili e una lista di quelli che verranno

sviluppati in futuro.

Decentralizzazione
Commercio.network assegnerà la
Transazioni fra aziende private: le imprese potranno

governance in modo che i partecipanti al a rete non debbano raggiungere il massimo livel o di privacy in Commercio.

affidarsi a un’entità centrale per gestire

le proprie transazioni.

network formando col egamenti privati che consentonoi

transazioni private.

Accesso immediato: le aziende potranno sfruttare

la Blockchain da subito invece di sviluppare da zero **Scalabilità e prestazioni:** grazie al consenso del a Proof of

un'implementazione a Blockchain.

Stake (PoS) e ai limiti di tempo di blocco basso, la rete federata

Commercio.network potrà superare la rete pubblica, come

Ethereum o Bitcoin e scalare fino a centinaia di transazioni al

Sotto-reti autorizzate: Commercio.network consentirà al e secondo o più.

aziende di formare sotto-reti attraverso connessioni private

(chiamate Pairwise) in cui solo i membri di tali reti possono

accedere al e informazioni condivise.

Finalità istantanea: il meccanismo di

consenso chiamato

Tendermint, garantisce l'immediata finalità del e transazioni.

68

Incentivi criptoeconomici: la componente criptoeconomica **Libertà e Interoperabilità:** le aziende che utilizzano

di Commercio.network consentirà al e aziende di sviluppare Commercio.network non sono bloccate nel 'ambiente IT

meccanismi che disincentivano le attività sgradite e creano di un singolo

fornitore. Commercio.network attraverso il

ricompense per le attività gradite.

protocol o IBC di Cosmos.network potà essere col egata a

qualsiasi altra Blockchain presente e futura.

Tokenizzazione: le aziende potranno certificare su

Commercio.network qualsiasi docomento di credito o debito **Open source:** la tecnologia e le sorgenti di Commercio.

che è stato scambiato in formato digitale.

network sono totalmente open source e possono essere

ispezionate da chiunque lo voglia su GitHub.

Standard: Commercio.network sarà basata su standard ISO

ed è in programma di raggiungere la conformità europea

eIDAS .

100 possibili usi per la Blockchain

Ledra Capital, società di venture capital con sede a New York, ha elencato una gamma

di potenziali utilizzi della tecnologia Blockchain.

Alcune di queste categorie includono strumenti finanziari, documenti pubblici, privati

e semi-pubblici, chiavi fisiche, intangibili e altre potenziali applicazioni.

Strumenti finanziari, registri e

Certificati di nascita

Dati sul genoma

Licenze per musica/film/libri

modelli

Certificati di morte

Percorsi GPS (istituzionali)

(DRM)

Valuta

Tessere elettorali

Documenti di consegna

Domini web

Private Equity

Elezioni

Arbitrati

Identità online

Azioni di aziende quotate

Ispezioni sanitarie/sicurezza

Obbligazioni

Permessi di costruzione

Chiavi fisiche delle risorse

Altro

Derivati (futures, forward, swap,

Porto d’armi

Chiavi di casa/appartamento

Documenti probatori (foto, audio,

opzioni)

Sentenze Tribunali

Chiavi di casa vacanza/

video)

Diritti di voto

Atti giudiziari

condivisione a tempo parziale

Record di dati (punteggi sportivi,

Commodity

Registrazione delle avvenute

Chiavi delle camere d’albergo

temperature, catena del freddo,

Registri pubblici di spesa

votazioni

Chiavi auto

ecc.)

Registri pubblici di trading

Registrazioni atti Non Profit

Chiavi per auto a noleggio

Schede SIM

Registri pubblici di mutui/prestiti

Contabilità dello Stato /

Chiavi auto in leasing

Identità della rete GPS

Registri pubblici di manutenzione

trasparenza

Chiavi dell’armadietto

Codici di sblocco armi

Contratti di Leasing

Chiavi di sicurezza

Codici di lancio nucleare

Servizi assicurativi

Registri privati (anonimizzati)

Consegna dei pacchi (Multisig tra

Antispam (micropagamenti per

Crowdfunding

Contratti

impresa trasporti e destinatario)

l’invio di posta)

Microfinanza

Firme

Record scommesse

Car sharing

Microcarità

Testamenti

Record di eSport

Gestione energia e consumi

Fiduciarie

Record di FantasySport

Lista nozze

Pubblici registri

Escrow

Tracciamento filiera

Titoli dei terreni

Percorsi GPS (personali)

Immobilizzazioni immateriali

agroalimentare

Atti Notarili

Buoni

Testamenti ed eredità

Registri dei veicoli

Registri semi-pubblici

Coupon

Controllo di sigilli ed etichettature

Licenze commerciali

(anonimizzati)

Voucher

...

Costituzione/scioglimento di

Diplomi di laurea

Tessere associative

imprese

Certificazioni

Prenotazioni (ristoranti, hotel,

Registri soci dell’azienda

Attestati di corsi professionali

code uffici, ecc.)

Gazzetta Ufficiale

Voti scolastici

Biglietti per i film

Casel ario giudiziario

Risorse umane (cedolini paghe,

Brevetti

Passaporti

CUD)

Diritti d’autore

Patenti auto

Documentazione medica

Marchi di fabbrica

Patenti nautiche

Registri contabili

Licenze Taxi

Brevetti di volo

Scambio di documenti

Licenze software

Carte di identità

commerciali

Licenze per videogiochi

71

03

Capitolo terzo

Finanza con la Blockchain

Dai Token aziendali ai pagamenti Smart

FARE **Business** CON LA **Blockchain**

Capitolo terzo

Finanza con la Blockchain

Dai Token aziendali ai pagamenti Smart

Moneta legale e Criptovaluta

strumento di pagamento non coperto da riserve di altri

materiali (ad esempio: riserve auree) e quindi, privo di valore

Quando si inizia una conversazione sul a Blockchain si finisce intrinseco. Questa

moneta viene definita legale grazie al fatto

invariabilmente nel tema del e Criptovalute e altrettanto che esiste uno Stato sovrano che sancisce questo valore.

rapidamente ci si ritrova a discutere di Bitcoin. Proviamo a

dare un'occhiata più nel dettaglio al e Criptovalute e a come Gran parte del a valuta legale in circolazione, quel a che gli

si relazionano al a Blockchain.

economisti definiscono M2 e M3, è

digitale. Non esiste in

forma di banconota di carta o di moneta metal ica, ma è in

Prima di parlare di Criptovalute, parliamo di valuta detta forma di valuta elettronica, cioè una transazione scritta in

anche valuta legale o moneta fiat. La valuta fiat è uno un libro mastro gestito da un database centralizzato di una

Banca. Se un'organizzazione abbastanza grande (ovvero La grande differenza del e Criptovalute rispetto al e valute

una col ettività) emette, usa e accetta qualcosa come fiat, il cui valore è sostenuto dal governo che le emette, è che

pagamento, automaticamente quel qualcosa acquisisce non esiste un organo di governo centrale. Quando è stato

valore, dato che è riconosciuto come mezzo di scambio e può creato Bitcoin, la prima e più famosa Criptovaluta, è stato

essere considerato a tutti gli effetti una moneta.

previsto nel protocol o un' emissione limitata a 21 milioni di

monete.

Una Criptovaluta è essenzialmente valuta elettronica, cioè

una transazione scritta in un libro mastro gestito da un' entità Queste Criptovalute, di solito, vengono messe in circolazione

decentralizzata, ovvero una col ettività di persone. Quindi gradualmente, seguendo una regola di emissione predefinita

le Criptovalute sono del e basi monetarie indipendenti, nel protocol o stesso del a moneta e non più modificabile.

esattamente al a stesso livel o del e monete di uno Stato Una volta che tutti i Bitcoin saranno stati estratti, non

sovrano. Possono essere cambiate in un "Money Exchange" verranno più messe in circolazione altre monete. Si prevede

digitale al o stesso identico modo in cui si cambiano Euro che il 100% dei Bitcoin sarà reso disponibile entro il 2140.

con Dol ari e viceversa.

La nascita dei Token

di mercato superiore ai dieci milioni di dol ari.

Tempo fa in Italia, prima del ’avvento del a telefonia mobile, Mentre queste Criptovalute sono ancora molto piccole

esistevano le cabine telefoniche dove le persone potevano in termini di quota di mercato rispetto al e valute

fare una telefonata attraverso l’uso di un gettone (Token). fiat, esse continuano ad evolversi e a diffondersi.

Lo stesso gettone poteva essere utilizzato in certe occasioni ***Non c’è dubbio che il denaro, così come lo conosciamo,***

anche per comprare un gelato, a testimonianza che il valore può ***cesserà di esistere. Probabilmente ci vorrà più***

comunque essere dato dal a comunità e non solo da uno Stato.

di un decennio, ma potrebbe accadere prima.

La nascita di Ethereum nel 2015 ha permesso a chiunque di Pensateci: come usate il contante oggi? Con i nostri smart-

generare del e Criptovalute utilizzando gli strumenti degli phone possiamo utilizzare sistemi tipo WeChat, Apple Pay

Smart Contract. Da al ora sono emersi diversi standard o Google Pay per pagare le cose di uso quotidiano che un

di Token, di cui il più famoso è l'ERC20 e sono state create tempo venivano acquistate solo in contanti, come il caffè che

numerose Criptovalute con diversi scopi. Al momento si prende andando al lavoro.

del a pubblicazione di questo libro sono disponibili

oltre duemila valute criptografiche e alcune decine di

esse hanno addirittura raggiunto una capitalizzazione

Tipologie di Token

Secondo la SEC americana e la FINMA elvetica, che sono le due

autorità finanziare più interessate al fenomeno del e Criptovalute, ci

sono cinque principali tipologie di Token e altre permutazioni ibride

fra di esse:

- **Payment Token**

Criptovaluta tipo Bitcoin o Ether descritta nei paragrafi precedenti.

- **Security/Asset Token**

Rappresentazione di asset finanziari.

- **Utility Token**

“gettoni telefonici” che danno diritto ad un servizio.

- **Non Fungible Token**

Token che rappresentano un asset unico e non sostituibile.

- **Stable Coin**

è un token che vale sempre 1€ o 1$ o un valore fisso.

Token

Expert

ATTENZIONE!!!

A seconda del tipo di Token, i creatori e gli acquirenti di

un token possono avere diritti e responsabilità diversi: è

necessario consultare un legale esperto in materia prima di

intraprendere qualsiasi azione.

Security Token

intermediari (banchieri, ecc.). I Security Token eliminano,

nel a maggior parte dei casi, la necessità di affidarsi a dei

I Security Token sono beni digitali soggetti al e stesse regole banchieri, il che riduce le commissioni e gli Smart Contract

finanziare che vengono adottate dai prodotti finanziari offerti potranno, un giorno, diminuire anche la dipendenza dagli

al pubblico. In termini semplici, sono l'intersezione dei beni avvocati. Questi Smart Contract, inoltre, ridurranno la

digitali (Token) con i prodotti finanziari tradizionali. Si tratta complessità, i costi e la burocrazia nel a gestione dei titoli

di una nuova tecnologia che migliora un vecchio prodotto.

(raccolta firme, trasmissione dei fondi, distribuzione degli

Se Bitcoin viene considerato una valuta digitale, al ora utili etc).

possiamo considerare i Security Token del e azioni digitali **Esecuzione più**

rapida dello scambio: più persone sono

di una azienda. Questo significa che qualsiasi bene la cui coinvolte in uno scambio, più tempo ci vuole per eseguirlo.

proprietà dà diritto ad una rendita (asset) può essere e sarà Quando i Security Token rimuovono gli intermediari dal e

tokenizzato (azioni di società pubbliche, quote di società operazioni di investimento, consentono agli emittenti di

private, titoli di debito, titoli di credito, beni immobili, ecc).

offrire, con successo, i loro titoli. Inoltre, il regolamento

Perché sono importanti i Security Token?

immediato del e negoziazioni sul mercato secondario per i

Security Token, diventerà un vantaggio interessante anche

I Security Token apportano una serie di miglioramenti ai per gli emittenti e gli investitori.

prodotti finanziari tradizionali, rimuovendo l’intermediario

dal e transazioni di investimento (di solito un banchiere). **Esposizione al libero mercato:** la maggior parte del e

La rimozione degli intermediari porta a commissioni più operazioni di investimento oggi non sono esposte ad una

basse, esecuzione più veloce del e operazioni di scambio, base globale di investitori. Ad esempio, è difficile per gli

esposizione al libero mercato, maggiore base di potenziali investitori in Asia investire in società private italiane o in

investitori, funzioni di servizio

automatizzato e mancanza di beni immobili. Con i Security Token, i proprietari di asset

manipolazione degli istituti finanziari.

potrebbero semplicemente promuovere le loro offerte a

chiunque abbia una connessione internet (entro i limiti

Commissioni più basse: molte commissioni associate al e normativi). Questa esposizione al libero mercato dovrebbe

transazioni finanziarie derivano da pagamenti dovuti agli portare a un

cambiamento significativo nel e valutazioni

78

degli asset, poiché qualsiasi asset che non è esposto al libero **I Security Token sono conformi alla legge?**

mercato non viene valutato correttamente.

Consulta un avvocato! Questo libro non è un parere legale

Base più ampia di investitori: quando i proprietari di perché l'autore non è un avvocato. Se i Security Token

beni possono presentare offerte a chiunque abbia una vengono emessi rispettando le leggi e i regolamenti in

connessione internet nel mondo, la base potenziale di materia di emissione e vendita di prodotti finanziari, essi

investitori aumenta drasticamente. Ad esempio, preferireste possono essere considerati legali. In ogni caso il valore

mostrare la vostra opportunità di investimento solo a maggiore è la rimozione del e istituzioni finanziarie e degli

investitori e istituzioni italiani accreditati o a tutti i potenziali

intermediari, non certo quel o di cercare di rimuovere le

investitori nel mondo? La concorrenza è sana e rappresenta regole a protezione degli investitori.

un bene assoluto a lungo termine per i mercati finanziari.

L'emissione e l'acquisto di Security Token sono soggetti al e

Funzioni di servizio automatizzate: gli avvocati sono meno norme federali americane sui titoli e a al e regole di condotta

intermediari e più fornitori di servizi nel

a maggior parte del e del a FINMA elvetica: nel a comunità europea e in Italia in

transazioni. Con i Security Token gli emittenti inizieranno particolare non esiste alcuna legislazione a riguardo.

ad utilizzare Smart Contract per automatizzare la funzione

di fornitore di servizi attraverso il software. Questo non

significa che gli avvocati scompariranno, ma piuttosto che il

loro ruolo sarà più consultivo.

Mancanza di manipolazione delle istituzioni finanziarie:

questo è un argomento complesso e sicuramente

controverso. Brevemente, la probabilità di corruzione e di

manipolazione da parte degli istituti finanziari diminuisce se

questi ultimi vengono rimossi dal processo di transazione di

investimento.

Utility Token

Si tratta di un gettone non fisico. Pensate ad un gettone

telefonico che non potete toccare o tenere in mano, ma che

vi viene accreditato, se consegnate dei soldi al fornitore o

a un suo intermediario. Questo significa che l'acquirente di

un Utility Token ha pagato l'emittente del Token in modo

che l'azienda possa utilizzare il prodotto o il servizio da esso

fornito.

Crowdfunding: un altro caso più interessante è il

Crowdfunding, dove un'azienda vende un Utility Token di un

prodotto che deve ancora sviluppare e il cliente comprandolo

fornisce al 'azienda le risorse finanziare necessarie per

sviluppare il prodotto che l'acquirente del Token potrà

utilizzare quando quel bene o servizio verrà lanciato.

ICO: dal 2016 al 2018 le startup sul a Blockchain hanno

raccolto 5,4 miliardi di dol ari attraverso del e Initial Coin

Offering (ICO). Una ICO è il processo in cui degli Utility Token

vengono emessi e venduti in modalità Crowdfunding. Perché

le persone hanno acquistato questi Token se non possono

riscattarli in cambio di un prodotto o servizio? Anche se non

è possibile riscattare un Utility Token

per beni o servizi, un

proprietario di Utility Token può andare su un Digital Money

Exchange (si pensi a entità tipo una borsa) per comprare e

vendere Utility Token.

Non-Fungible Token (NFT)

Smart Contract che è conforme ad uno standard chiamato

ERC-20. Per semplicità, immaginiamo che ognuno di questi

Esiste una categoria completamente diversa di Token Token sia una banconota da 10 Euro. Se si invia un Token

chiamati NFT, acronimo di Token non Fungibili. Cosa significa a qualcuno e, se ne riavrete un altro una settimana dopo,

“non fungibile”? Quando qualcosa è fungibile - in questo saranno identici.

caso un Utility Token, un Security Token o un Payment Token

- significa che può essere facilmente sostituito da qualcosa di Tutto questo cambia con Token non Fungibili, molti

dei quali

identico ed è totalmente intercambiabile. Nel mondo reale sono conformi ad uno standard chiamato ERC-721. Questi

qualcosa di fungibile è una moneta da 1€ che hai in tasca: possono essere paragonati ad un opera d’arte , nel senso che,

se doveste prestare quel a moneta a qualcuno, non sarebbe ogni opera d’arte ha caratteristiche uniche e livel i variabili di

importante se non restituisse esattamente lo stesso Euro. rarità. Se si dovesse accidentalmente prestare una di queste

Le cose cambiano se qualcosa non è fungibile. Anche se due opere d'arte o Token a qualcuno, che vi restituisse un'opera

elementi possono sembrare identici a colpo d'occhio, ogni d'arte o Token diversi, non sareste contenti.

elemento avrà informazioni uniche o attributi che li rendono

insostituibili o impossibili da scambiare. Un esempio fisico

di un bene non fungibile potrebbe essere un biglietto

aereo. Ogni biglietto ha lo stesso aspetto

degli altri biglietti,

ma ciascuno ha scritto sopra il nome del passeggero, la

destinazione, l’orario di partenza e il numero preciso di posto

dove andarsi a sedere. Scambiare questo biglietto con uno

$

sconosciuto porta gravi conseguenze, come finire a migliaia

di chilometri di distanza da dove volevate andare, qualora la

sicurezza aeroportuale non vi blocchi prima.

La maggior parte dei Token Fungibili (Utility, Security e

Payment) vengono generati su Ethereum utilizzando uno

Uno dei pionieri dei Token non fungibili è stato CryptoKitties.

Co, un'applicazione su Ethereum dove i giocatori hanno la

possibilità di collezionare e allevare gatti digitali. Se avete

avuto un gatto, sapete che non sono facili da sostituire

perché il loro aspetto e la loro personalità li rendono unici.

In questo caso, CryptoKitties ha replicato questo concetto

nel mondo della Blockchain con il materiale genetico

digitale di ogni gatto immagazzinato in un Token NFT.

Questi Token/Gatto possono essere acquistati e venduti

su Ethereum, e alcuni sono più rari di altri. Infatti, le

vendite nel 2017 hanno raggiunto i 12 milioni di dollari con

il CryptoKitty più costoso che è stato venduto a 120.000

dollari.

Esistono migliaia di casi di utilizzo per i Token NFT: pensate

a garanzie su prodotti, certificati di proprietà, certificati di

origine e moltissimi altri citati precedentemente.

Commercio.network ha intenzione di rendere disponibile

al e aziende un sistema per generare Token NFT in modo

semplice e veloce. Immaginate di poter tokenizzare i vostri

crediti creando un Token NFT di una fattura, e ottenere

liquidità in tempi rapidi cedendo il credito ad una terza parte

su un Exchange di Token NFT.

Stable Coin

Quando nel 2008 lessi il whitepaper di Satoshi Nakamoto Gli utenti tendono ad ignorare le soluzioni che ignorano le

mi resi conto che aveva definito una visione possibile per esigenze degli utenti.

un futuro decentralizzato. A distanza di qualche anno, oggi Gli Stable Coins sono più vicini al e aspettative degli utenti,

la Blockchain è ancora qualcosa per pochi. Cosa manca per che quando comprano 10€ di crediti per una ricarica

fare sì che tutti la usino? La risposta sono gli Stable Coins. telefonica si aspettano di avere 10€ anche domani e non

Uno Stable Coin è un token che vale sempre 1€, 1$ o un avere in conto 8€ o 12€ a causa del cambio.

valore fisso.

Gli Stable Coins come il DAI prodotto da MakerDAO associato

al Dol aro e il CashCoin prodotto da Commercio.network

Oggi le soluzioni basate sul a tecnologia del a Blockchain associato al ’Euro,

sono criptovalute basate su meccanismi

obbligano gli utenti a:

criptoeconomici avanzati che le ancorano al a valuta Fiat.

• Registrarsi su degli Exchange per ottenere dei Token.

• Dover attendere del tempo per ottemperare alle regole

di registrazione e antiriciclaggio.

• Utilizzare delle procedure complesse di creazione degli

account.

$

• Rischiare di perdere il denaro per sempre quando si

dimentica la password.

• Subire il rischio di cambio di una moneta che fluttua

anche del 30% al giorno.

Exchange di Token e Criptovaluta

I vantaggi di un DEX rispetto ad un CEX sono:

Ci sono due tipi di scambio di Token oggi in funzione: gli • Un DEX può essere più resistente al ’hacking di un CEX

exchange centralizzati CEX e gli scambi decentralizzati DEX.

perché le informazioni sul conto non sono condivise

con l’operatore del o scambio: i fondi potrebbero essere

Exchange centralizzato (CEX) funziona come una classica

tenuti sul vostro conto e voi sarete l’unica persona con

borsa di intermediazione: si depositano i fondi in un conto

accesso.

e la borsa fa le compravendite per voi. Il vantaggio è che

l'Exchange fa tutto il lavoro, ed è spesso assicurato e • Teoricamente, i governi o le autorità di regolamentazione

regolato dal e autorità. La maggior parte degli Exchange,

non possono spegnere un DEX perché è decentralizzato,

tipo COINBASE e BINANCE, sono

centralizzati. Un vantaggio

operando attraverso un'ampia varietà di nodi.

per questi Exchange è che accettano pagamenti con carta • Un DEX opera su tutto il cloud attraverso una varietà di

di credito o di debito e bonifici bancari. Possono anche

nodi e non c'è un singolo server che possa essere bloccato

pagare in valuta fiat, come dol ari o euro, che molti utenti

o violato.

preferiscono.

• Su un DEX c’è un più alto grado di privacy perché non si

Exchange decentralizzato (DEX) è un mercato per le

condividono i dati con l’operatore.

Criptovalute e per i Token che è aperto a tutti. Nessuno ha

il control o di un DEX; la gente acquista e vende su base • Su un DEX mantenete il control o dei vostri fondi sul vostro

individuale tramite applicazioni di trading Peer-to-Peer. Un

conto personale.

modo di pensare ad un DEX è come una soluzione di trading • Un DEX può essere più veloce perché si fanno le operazioni

“fai-da-te”: effettuate le operazioni, i fondi si spostano dal

da soli.

vostro conto. Il più grande vantaggio di questo sistema è

che i vostri fondi non dovranno mai essere affidati ad una

società di trading o ad altre terze parti e

rimarranno sempre

nel wal et del a persona che effettua la transazione. Questi

Exchange operano esclusivamente con moneta digitale.

84

85

Gli svantaggi di un DEX rispetto ad un CEX sono:

Sulla Blockchain di Commercio.network esiste un modulo

chiamato CommercioDEX che

permetterà di fare trading

• I fondi non sono regolamentati o assicurati. Gli scambi ***di Token Fungibili e non Fungibili, attraverso un wallet au-***

regolamentati potrebbero essere tenuti a restituire il ***togestito, utilizzando un protocollo su Ethereum chiamato***

denaro in qualsiasi momento, in modo da mantenere i ***0x.com tramite cui si accede ad un pool mondiale di liquidi-***

fondi in deposito a garanzia per prelievi rapidi.

tà e di utenti interessati a scambiare Tokens.

• La maggior parte dei DEX non accetta pagamenti con

carta di credito, di debito o bonifico bancario.

• Il volume degli scambi è limitato, il che può mantenere i

prezzi bassi e le commissioni elevate.

• I servizi disponibili dai DEX sono limitati: Margin Trading,

Stop Loss e operazioni che coinvolgono le valute fiat non

vengono offerte.

CEX

• Potrebbe non esserci un servizio clienti da contattare

quando c’è un problema.

• Un DEX può essere molto più costoso di un CEX perché

potrebbe essere necessario acquistare Ethereum Gas

(ETH) ogni volta che si effettua una transazione.

DEX

Pagamenti Smart

che il destinatario può richiedere i fondi presentando

una pre-immagine valida del digest di hash prima di una

Un pagamento Smart, che avviene tramite un contratto *determinata scadenza (timeout). Dopo il timeout, i fondi*

Hashed-Timelock (HTLC), è un

trasferimento di *vengono automaticamente restituiti al mittente.*

Criptovaluta in cui la condizione di pagamento è applicata

dalla Blockchain. Si tratta di un concetto originato Gli HTLC vengono fatti rispettare dal a Blockchain, quindi le

nel ’ambito del a comunità Bitcoin che viene applicato su parti che effettuano le transazioni devono solo fidarsi che

Lightning Network e può essere utilizzato su Ethereum, nel e la Blockchain esegua correttamente il contratto, (non del a

sidechain (L2) e nel modulo CommercioPay nel a Blockchain controparte.) Si può anche prevedere che gli HTLC possano

di Commercio.network.

essere eseguiti su diverse Blockchain e addirittura senza la

presenza di una Blockchain, con degli Agreements (HTLA).

Quando il trasferimento è "preparato", i fondi del mittente

sono messi in attesa dal registro dell'avverarsi di una

condizione predefinita. La condizione è un Hashlock.

Un Hashlock o il digest di una funzione di hash criptografico,

come SHA-256, è un tipo di impedimento che limita la spesa

di un output fino a quando un dato specifico non viene

rivelato pubblicamente. Gli Hashlock hanno l'utile proprietà

che, una volta che un Hashlock è reso pubblico, qualsiasi

altro Hashlock protetto dal a stessa

chiave, può anch'esso

essere aperto. Questo permette di creare output multipli che

sono tutti gravati dal o stesso Hashlock e che diventano tutti

spendibili al o stesso tempo.

Il timelock è un impedimento temporale, come una

cassaforte a tempo, dove lo Smart Contract stabilisce

Pagamenti Condizionali

Due parti che utilizzano un HTLA su una Blockchain che Il destinatario deduce quindi l'importo di ogni "trasferimento

non supporta Hashlock e Timeout potrebbero procedere condizionale" eseguito dal 'importo pre-finanziato. In questo

nel modo seguente: il mittente invia un messaggio caso, il mittente deve fidarsi che il destinatario non rubi

al destinatario dicendogli che vuole "preparare" un l'importo pre-finanziato, ma questo rischio può ovviamente

trasferimento con un determinato Hashlock e Timeout. Le essere ridotto limitando l'importo pre-finanziato.

parti concordano che, se il destinatario presenti la pre-

immagine dell'hash prima del Timeout, il trasferimento Gli HTLA funzionano quindi con Blockchain che supportano

viene eseguito e il mittente deve il denaro al destinatario.

Hashlock e timelock (come HTLC) e con Blockchain che non

I debiti vengono saldati tramite

semplici trasferimenti sulla li supportano.

Blockchain.

Sul a Blockchain di Commercio.network esiste un modulo

chiamato CommercioPAY che permette di fare pagamenti

Nel caso di un accordo post-finanziamento, il mittente tracciabili utilizzando un sistema HTLA e un sistema

può saldare il proprio debito con il destinatario per ogni trasparente di rating sul ’affidabilità creditizia dei

membri

pagamento, se la sua Blockchain è veloce e ha commissioni del a rete chiamato CommercioSCORE.

basse, oppure una volta che l'importo totale dovuto

raggiunge il limite di credito del e parti. In questo caso, il

destinatario deve affidarsi al mittente che paghi quanto da

lui dovuto. Il rischio può essere ridotto limitando la quantità

di denaro che il mittente può inviare

prima del pagamento.

Per gli accordi pre-finanziati, il mittente trasferisce al

destinatario l'importo di un singolo pagamento o un importo

ingente e beneficia del 'equivalente di una linea di credito.

CommercioPAY

Diversi tipi di pagamenti Smart

I vari tipi di pagamenti Smart presentano un compromesso tra

complessità e rischio. Più funzionalità offre una Blockchain,

meno rischioso sarà per gli utenti fidarsi uno dell'altro.

Canali di pagamento

Depositi Escrow

Canali di pagamento

Linee di credito

condizionali

(con HTLCs)

semplici

(con HTLC)

Supporto della

Alto

Alto

Medio

Basso

Blockchain

Complessità

Alto

Medio

Basso

Basso

implementazione

Rischio Bilaterale

Basso

Basso

Medio

Alto

89

04

Capitolo quarto

Acquisti e vendite con la Blockchain

Dal EDI al ’e-commerce B2B 3.0

FARE **Business** CON LA **Blockchain**

Capitolo quarto

Acquisti e vendite con la Blockchain

Dal EDI al ’e-commerce B2B 3.0

Il commercio internazionale è veramente “vecchia scuola”, sostanziale nuovo livel o di qualità di gestione dei processi

c’è poca tecnologia. Ci sono ancora pezzi di carta spediti in aziendali commerciali, al fine di:

giro per il mondo per accompagnare gli scambi commerciali e • **Ridurre gli errori:** l’intero processo di ordine è prono

le spedizioni ed è fondamentalmente attivo lo stesso sistema

al ’errore e migliaia di documenti cartacei e scritte a

in vigore dal ’epoca del mercantilismo del XVI secolo.

penna sono spesso mal interpretati.

Dagli anni 80 esistono dei sistemi chiamati EDI (Electronic • **Ridurre i tempi di consegna:** quando si esegue

Data Interchage) che vengono utilizzati per scambiare

un ordine digitale l'azienda può consegnare più

documenti, ma questi sistemi sono orientati e creati su

velocemente, riducendo anche il relativo tempo di Order

misura dei loro proponenti, cioè grandi aziende in specifici

to Cash.

settori economici (GDO, Automotive, Aerospace).

• **Eliminare i costi di inserimento dati:** quando tutto

Sebbene questi sistemi di scambio di documenti

viene scambiato digitalmente, l'immissione manuale non

rappresentino un grande passo avanti verso la digitalizzazione

è più necessaria e si riducono i tempi e i costi.

del commercio, non sono altro che un primo passo su un più

lungo cammino.

• **Migliorare la tracciabilità:** quando tutto avviene

digitalmente, le transazioni sono contabilizzate e

Possiamo sperare che tra qualche anno, grazie al a

qualsiasi errore può essere tracciato al punto di origine.

Blockchain, assisteremo al a nascita di servizi che offrono

soluzioni “end-to-end” per la Supply Chain.

Questo nuovo tipo di entry point di scambi commerciali

documentali end-to-end del a Supply Chain offriranno un

Standardizzazione dei documenti

digitali

Una sfida enorme del a Blockchain è rappresentata dal fatto

di utilizzare un formato comune di dati

per lo scambio di

informazioni tra gli attori di una Supply Chain. Da molti anni

l'industria del a Supply Chain lotta contro l'insufficiente

standardizzazione EDI che si traduce in un suo funzionamento

inadeguato su base globale.

La soluzione a questo problema non è di creare un nuovo

standard, ma di essere aperti a diversi standard, anche se

pensiamo che lo standard emergente sarà UBL 2.1 che verrà

utilizzato dal 2020 come standard europeo eIDAS[3], e oggi

viene parzialmente già impiegato in Italia per la fattura

elettronica B2B.

eIDAS

3 Regolamento UE n° 910/2014 - eIDAS (si veda: https://www.agid.gov.it/

it/piattaforme/eidas)

EDI nel passato

Oggi sono in uso diversi standard EDI, tra cui:

Electronic Data Interchange (EDI) è lo scambio di

• UBL 2.1

documenti aziendali da computer a computer in un

formato elettronico standard tra partner commerciali.

• UN/EDIFACT i

I documenti EDI possono essere

trasferiti dal software

• **ANSI ASC X12**

gestionale di un’azienda a quel o di un’altra azienda.

• **GS1 EDI**

L’inserimento di una fattura elettronica, ad esempio, può

avvenire immediatamente, senza il coinvolgimento manuale

• **TRADACOMS**

del e persone che ral enterebbe l’elaborazione dei documenti

• **ODETTE**

e potrebbero introdurre errori.

• **VDA**

I documenti commerciali più comuni scambiati tramite EDI

sono gli ordini di acquisto, le fatture, gli avvisi di spedizione

• **HL7**

la polizza di carico, documenti doganali, documenti di

inventario, documenti di stato di spedizione e documenti di

pagamento.

Sfortunatamente per ognuno di questi standard ci sono

molte versioni diverse. Questo comporta che quando due

imprese decidono di scambiare documenti EDI, devono

necessariamente concordare lo standard e la versione EDI

specifici. Le imprese in certi casi utilizzano un traduttore

EDI per convertire i documenti aziendali in un formato EDI

accettato dal ’applicazione.

EDI

94

UBL 2.1

UN/EDIFACT i

ANSI ASC X12

GS1 EDI

TRADACOMS

ODETTE

VDA

Necessità di collaborazione

Questo approccio andava molto bene negli anni 80, ma

riteniamo che EDI non possa supportare i complessi processi

di Supply Chain di oggi, in quanto il trasferimento dei dati tra

i vari sistemi ERP genera situazioni potenzialmente critiche.

Ecco una lista di problemi che sorgono

anche in sistemi EDI

molto stabili.

Clienti e fornitori hanno bisogno di una visione condivisa

della situazione reale della fornitura sulla Blockchain,

consentendo loro di risolvere in modo collaborativo i

problemi identificati e, in tal modo, di evitare costosi colli

di bottiglia.

La Blockchain con i sui incentivi

criptoeconomici può

diventare la rete di scambio per fare sì che le aziende che

partecipano al network interagiscano l'una con l'altra in

modo semplice, economico e sicuro.

96

Necessità di fiducia

Trasparenza e collaborazione: documentazione a prova di

manomissione che certifica il percorso del prodotto lungo

Una chiave di successo del a col aborazione globale tra tutta la Supply Chain e la condivide con le parti interessate.

aziende si basa sul a fiducia. La fiducia sul a Blockchain si Il sistema funziona senza un repository centrale o un

ottiene dai processi trasparenti che permettono di facilitare, amministratore singolo (decentralizzato).

control are o far rispettare lo scambio certificato di un

documento, e che rendono superflua qualsiasi verifica. Lo **Scalabilità e disponibilità:** in particolare le sidechain

(L2)

scambio di un documento basato sul a Blockchain viene stanno risolvendo i problemi di scalabilità per le transazioni

eseguito tramite un sistema di firma elettronica verificabile di scrittura. Tutte le persone nel mondo possono accedere

da tutti gli utenti.

via internet ai set di dati distribuiti e rindondanti memorizzati

(distribuiti).

La Blockchain crea un sistema di fiducia decentralizzato

portando i seguenti vantaggi:

Sicurezza e Privacy: un nodo non deve necessariamente

rivelare l'identità fisica del a persona o del 'organizzazione e

il documento commerciale può avere una firma digitale con

chiavi criptografiche private (immutabilità).

Commercio.network, per esempio, vuole creare una

rete dove le imprese possono scambiarsi documenti

commerciali in piena sicurezza attraverso la Blockchain.

La somma di ogni singolo passaggio di documenti crea

un valore più grande, perché attraverso un processo

trasparente di co-certificazione valida i crediti e debiti di

tutte le parti in gioco.

La Blockchain dei Documenti

Commercio.network è una Blockchain

Federata,

• Scambiarsi documenti attraverso un sistema che

aperta a 250 milioni di imprese , che aiuta a

certifichi sia l'identità delle parti coinvolte, sia

scambiare documenti. Nel lungo periodo, può

la transazione.

inoltre aiutare a costituire la base per creare

un sistema di fiducia fra le aziende, tale da

permettere lo sviluppo di nuove applicazioni

• Garantire l'integrità del documento e quindi la sua

Fintech, quali il finanziamento delle fatture delle

immutabilità.

aziende (factoring) tokenizzando le fatture sulla

Blockchain Pubblica di Ethereum.

• Creare una connessione sicura e non tracciabile fra due

aziende.

Commercio.network

• Criptare i documenti per permettere la lettura solo alle

è stata progettata per

parti coinvolte.

consentire alle aziende di:

• Firmare i documenti tramite Blockchain per attestarne

l’origine.

• Marcare temporalmente la transazione dei documenti

sulla Blockchain per una loro eventuale verifica futura in

carico ad una terza parte.

98

Attualmente la Blockchain riesce a sostenere piccole

stringhe di testo che servono semplicemente a registrare un

trasferimento di saldo tra due parti.

Come è possibile dunque

pensare di archiviare documenti di grandi dimensioni sul a

Blockchain? Dobbiamo rassegnarci al fatto che la Blockchain

possa gestire unicamente piccole stringhe di testo?

La soluzione più promettente oggi disponibile è **l'IPFS,**

o Interplanetary File System, creato da Protocol Labs.

Si tratta di un protocol o Peer-to-Peer in cui ogni nodo

memorizza una raccolta di file hash. Un client che vuole

recuperare uno di questi file, può accedervi semplicemente

attraverso l'hash del file stesso. L'IPFS quindi esegue la

ricerca attraverso i nodi e fornisce il file al client.

Si può pensare che sia simile a BitTorrent. Si tratta di un

modo decentralizzato di memorizzare e fare riferimento ai

file, ma fornisce maggior control o e si

riferisce agli hash di

file, consentendo interazioni programmatiche molto più

ricche.

99

IPFS

Ecco alcuni semplici diagrammi per vedere il flusso di lavoro

del ’IPFS.

XML

1. Alice vuole caricare una fattura

elettronica su IPFS.

2. Mette manualmente il suo file XML nella sua directory

di lavoro o utilizza le API per farlo in modo automatico.

3. Dice a IPFS che vuole aggiungere questo file, il quale

genera un indirizzo (hash) del file. i file in IPFS hanno

sempre prefisso “Qm..”.

4. Il suo file è disponibile sulla rete IPFS.

Ora supponiamo che Alice voglia condividere questo file

con il suo col ega Bob attraverso l'IPFS. Per fare ciò dovrà

IPFS

semplicemente fornire a Bob l'hash dal passo 3 il quale eseguirà

i passi da 1 a 4 in senso inverso così facendo egli è in grado di

recuperare il file nel a sua interezza.

XML

IPFS non garantisce la riservatezza a

meno che il

dato memorizzato su tale piattaforma non sia stato

preventivamente cifrato. Chiunque sia in possesso del ’hash

di un file può recuperare tale file da IPFS. I file contenenti

informazioni riservate o sensibili (ad esempio immagini,

cartel e cliniche, etc) non sono quindi adatti per essere

gestiti da IPFS.

Per fortuna, esistono strumenti a nostra disposizione che si **1. Alice vuole caricare un file XML su IPFS, assicurandosi**

combinano molto bene con IPFS per proteggere i file prima di **che solo Bob lo possa leggere "in chiaro".**

essere caricati in IPFS. La criptografia asimmetrica consente

di criptare un file con la chiave pubblica del destinatario **2. Salva il file XML nella sua directory di lavoro e lo cifra**

previsto, in modo che solo lui possa

decifrarlo quando lo **con la chiave pubblica di Bob.**

recupera con IPFS. Un utente malintenzionato che recupera

il file da IPFS non può fare nul a con esso poiché non può **3. Dice a XML che vuole aggiungere questo file criptogra-**

decifrarlo.

fato, il quale genera un hash del file cifrato.

Modifichiamo il nostro precedente diagramma di flusso di **4. Il file cifrato è disponibile sulla rete IPFS.**

lavoro in modo da includere la cifratura e la decifratura:

5. Bob può recuperarlo e decifrare il file poiché possiede

la chiave privata associata alla chiave pubblica che è

stata usata per cifrare il file.

IPFS

6. Non essendo in possesso della chiave privata di Bob e

non potendola evincere attraverso alcun algoritmo, un

eventuale malintenzionato non può decifrare il file di

Alice.

CommercioDOCS

101

Come può la Blockchain arricchire funzionalmente il Manteniamo la semplicità dei dati che è richiesta sul a

contesto fino ad ora rappresentato?

Blockchain, ma si arriva a sfruttare la proprietà di archiviazione

dei file Peer-to-Peer di IPFS e la

decentralizzazione del a

Premesso che ciò che occorre per scambiarsi Criptovaluta in Blockchain, unendo il meglio dei due mondi. Dal momento

una Blockchain consiste in tre fattori:

che abbiamo anche aggiunto il fattore sicurezza utilizzando

- **il mittente**

la cifratura asimmetrica El iptic Curve Digital Signature

Algorithm (ECDSA), otteniamo in modo molto elegante l’

• il destinatario

“archiviazione”, la criptografia forte e la condivisione di

• la quantità di Bitcoin (o Ether, o altra Criptovaluta/

grandi dati e file sul a Blockchain.

cryptoasset) da trasferire

Immaginiamo di poter memorizzare in ogni blocco i

riferimenti di un’offerta di vendita spedita ad un cliente.

Quando inviamo una nuova offerta di

vendita, creiamo

semplicemente un nuovo blocco che si riferisce a

un'immagine criptografata o a un PDF dell'offerta che si

trova in IPFS.

poiché

Mitten t ***t*** u

e tte queste tran

Qu s

a a

nti z ***t*** i ***à*** oni che compo

Des n

ti g

na o

ta no

rio

un

blocco sono organizzate in un albero di Merkle (Merkle

tree) e soggette ad un dispendioso calcolo di hash, usare

la Blockchain per memorizzare i file nei blocchi è del tutto

antieconomico.

IPFS, utilizzato in combinazione con la Blockchain, ci aiuta

a risolvere questo problema architetturale: invece della

quantità di Bitcoin (o Ether, ecc.) da trasferire, l'oggetto

della transazione consiste nell'hash del file IPFS.

Commercio.network, in essenza, è un sistema basato su • **Creare un paio di chiavi ECDSA.**

una tecnologia di criptografia forte, altamente complessa

e sofisticata, che in questo caso viene resa fruibile al • **Impostare IPFS.**

99% delle aziende del mondo semplificando il processo di • **Cifrare un documento commerciale con la chiave**

adozione attraverso un API che nasconde dietro le quinte

pubblica di un altro utente.

la complessità necessaria e presenta all'utente finale solo

i benefici.

• **Caricare il file criptografato su IPFS.**

Le aziende che aderiranno al nostro network federato • **Essere assolutamente sicuri che solo l'utente**

di aziende trusted avranno a disposizione un software e/o

destinatario possa decifrarlo e visualizzarlo.

un’ API che permetterà loro in modo semplice, veloce ed • **Permettere a chiunque di verificare che è stata fatta**

economico di:

una transazione senza rivelare il contenuto stesso del

documento.

Privacy sulla Blockchain

Vale la pena notare che non si tratta di un requisito assoluto

e che i soggetti non hanno il diritto

incondizionato di essere

Cancel are i dati una volta salvati sul a Blockchain è un “dimenticati”. Se l’organizzazione ha altre ragioni legittime

problema altrettanto rilevante. Un aspetto del a legge e legali - come indicato nel regolamento - per conservare

europea sul a privacy (GDPR) [4] che ha ricevuto grande e trattare i dati, i soggetti non hanno il diritto di essere

attenzione, è il “diritto di essere dimenticato”, delineato dimenticati. Tuttavia le eccezioni sono poche

rispetto al a

nel ’articolo 17 intitolato “diritto al a cancel azione” moltitudine di usi dei dati comuni nel a nostra vita quotidiana.

(“diritto al ’oblio”). In parole povere, “oblio” significa che

le organizzazioni devono cancel are completamente i ***Quindi, nello spirito del GDPR, in che modo Commercio.***

documenti contenenti i dati di un soggetto da tutti gli archivi ***network potrebbe assicurare che i dati vengano cancellati***

in ciascuna del e seguenti occasioni

da tutti i luoghi in cui vengono memorizzati o elaborati?

• Quando la persona revoca il proprio consenso.

La cancellazione completa dei dati non è un' opzione

spesso possibile ed è di fatto irrealizzabile in una

• Quando lo scopo per cui i dati sono stati raccolti è

Blockchain.

completo.

- **Quando è imposto dalla legge.**

L’utilizzo di una funzione di eliminazione standard non

sempre rimuove completamente i dati (pensiamo a backup,

backup dei backup, backup del cloud provider, dischi non

smagnetizzati). Anche se non compaiono nei registri o negli

indici dei file, i dati eliminati sono spesso ancora recuperabili.

Privacy sulla Blockchain

In questi casi, nonostante i migliori sforzi, la semplice

“cancel azione” non consente di raggiungere la conformità

con il GDPR. Per complicare il problema, nel XXI secolo i dati

4 Regolamento UE 2016 679 (si veda:https://www.garanteprivacy.it/web/

aziendali vengono costantemente condivisi tra fornitori,

guest/home/docweb/-/docweb-display/docweb/6264597)

partner, rivenditori e clienti.

Quando il consenso viene revocato o un contratto si estingue, al GDPR, dovrebbero col ocarle nel contesto del e loro

come fa un'azienda a garantire che i dati personali presenti più ampie esigenze di sicurezza. L'adozione di soluzioni di

nei propri documenti vengano adeguatamente cancel ati da criptografia non strutturate è il modo più rapido per finire

tutti questi diversi attori?

con silos di sicurezza onerosi che

complicano maggiormente

le cose.

Commercio.network è arrivato alla conclusione che la **La criptografia è lo strumento che opera sui documenti,**

cancellazione criptografica sia l'unico modo pratico per **ma il sistema di gestione delle chiavi di un'organizzazione**

garantire pienamente che i dati siano inutilizzabili ai **sarà il fattore principale per il successo futuro in termini**

***fini degli obblighi di cancellazione imposti dal GDPR*, di sicurezza e conformità.**

utilizzando una chiave definita da un algoritmo per renderli

illeggibili.

Il "diritto al 'oblio" non è un'esigenza così scoraggiante

come potrebbe sembrare a prima vista. Un uso ponderato

L'unico modo per riportare i dati criptografati in uno del a criptografia può aiutare le organizzazioni a rispettare i

stato leggibile è quello di fornire la chiave corrispondente desideri del e persone interessate e a preservare la privacy

a quella usata per cifrarli. Se tale chiave dovesse in qualsiasi scenario.

essere cancellata, sarebbe impossibile decriptare i dati

rendendoli nuovamente leggibili.

La Blockchain offre quindi al e aziende un livel o superiore

di flessibilità nel decidere come adempiere a tali obblighi.

La criptografia è il tipo di strumento che le organizzazioni

Login

possono applicare a diversi livel i del flusso di dati, dal a

creazione al a distruzione. Se fosse semplice come eliminare

un file, un'organizzazione potrebbe utilizzare una soluzione a

livel o di file system per criptare il file ed eliminare la chiave.

Quando le aziende considerano le loro esigenze connesse

05

Capitolo Quinto

Risorse umane con la Blockchain

Dal ’identità distribuita al e connessioni ZKs al a firma elettronica

FARE **Business** CON LA **Blockchain**

Capitolo Quinto

Queste attestazioni (accrediti) possono essere utilizzate a

scopo di convalida del ’identità nel a

misura in cui uno si fida

Risorse umane con la del soggetto accreditatore.

Blockchain

Alla base del nostro sistema nasce il concetto di Pairwise

Connection, che è la creazione di un "tunnel criptografico

di dati" fra due aziende che si conoscono e che hanno

Dal 'identità distribuita al e

la possibilità di stabilire un contatto

basato sulla

connessioni ZK al a firma

conoscenza reciproca nel mondo reale.

elettronica

Le premesse necessarie per creare un sistema di interscambio

di documenti commerciali è un'identità stabilita e verificata

in modo sicuro. Al fine di prevenire gli attacchi di rete comuni

(come gli attacchi Sybil), l'identità di ogni partecipante

deve essere adeguatamente stabilita con un disincentivo

elevato per chi voglia creare nuove false identità che

appaiano autentiche.

Commercio.network vuole creare un processo di identità

decentralizzato, basato su attestazioni di terze parti che si

fondano sulla tecnologia della Blockchain.

Problemi da risolvere

Per affrontare questi problemi, Commercio.network ha

pensato ad un nuovo processo di validazione dell'identità

Il metodo tradizionale del a gestione del 'identità ha un forte ***non supervisionato, completamente automatizzato e***

problema di centralizzazione.

decentralizzato chiamato CommercioID.

Commercio.network ha l'obiettivo di creare una piattaforma

decentralizzata aperta a 250 milioni di aziende nel mondo. In

un sistema decentralizzato è difficile identificare gli utenti di

cui ci si può fidare e sui quali il sistema può contare in modo

affidabile per la verifica di identità.

Nessuno può entrare a fare parte di Commercio.network se

non viene accreditato da un altro membro già accreditato.

E’ necessario creare per le aziende due tipi di firma

elettronica:

• **Personal Electronic Signature:**

firma elettronica persona fisica.

• **Company Electronic Seal:**

sigil o elettronico persona giuridica.

CommercioID è una componente fondamentale della

piattaforma di Commercio.network che nel breve periodo

aiuta a stabilire un'identità affidabile

e, nel lungo periodo

tramite i pagamenti avvenuti con CommercioPAY, può

costituire la base per creare un indice di affidabilità

(CommercioSCORE) delle aziende che fanno parte della rete

Commercio.network.

CommercioID consente al e aziende, che si scambiano

CommercioID

documenti e informazioni, di accreditare

di certificare

l'identità di un altro utente CommercioID e di marcare queste

informazioni sul a Blockchain per un loro riutilizzo futuro. Più

accrediti o attestazioni un'azienda avrà, più la sua identità potrà

essere ritenuta valida dagli altri partecipanti del a rete. Inoltre,

CommercioAUTH

clienti e fornitori di un'azienda possono aiutare tale azienda,

garantendo implicitamente per essa, la sua capacità di

agire in modo responsabile. Durante questo processo di

accreditamento, i clienti e i fornitori di un'azienda possono

anche attestare vari tratti identificativi del nome (o l'indirizzo

CommercioSIGN

di un'azienda) per contribuire a proteggere la rete dai fakers

e fornire ulteriori prove di identità per l'azienda in questione.

Questo permetterà nel lungo periodo di superare le

Certification Authorities Centralizzate in favore di un

CommercioDAO

sistema Peer-to-Peer.

110

Attestato di identità aziendale

Verifica dell'identità riutilizzabile e

decentralizzato

trasportabile

Le amministrazioni pubbliche, gli istituti di credito e le imprese ***Pubblicando tutti gli attestati storici di identità sulla***

private detengono attualmente la maggior parte dei dati di ***Blockchain, le aziende possono contribuire a costruire***

identità aziendale esistenti al mondo. Queste organizzazioni ***un'identità riutilizzabile che crei fiducia nel tempo,***

svolgono un ruolo fondamentale nel 'aiutare gli utenti a ***eliminando il bisogno di verificarlaper ogni***

transazione

entrare nel sistema CommercioID attestando l'autenticità ***con un nuovo attore finanziario.***

dei dati inviati dagli utenti. Un esempio potrebbe essere

un contratto di factoring dove i finanziatori specificano gli **Questo non solo può far risparmiare denaro in tutta**

attestati di identità di cui si fidano per l'accreditamento del **la rete di aziende finanziarie, ma può anche aiutare a**

potenziale cliente, ai fini di poter

completare il pagamento. **ridurre significativamente i tempi di accettazione delle**

Gli accreditatori possono quindi accettare di verificare le **identità, evitando la duplicazione del lavoro da parte**

informazioni relative al ’identità e fornire le proprie chiavi **dei team antifrode e di conformità nelle organizzazioni**

pubbliche in risposta, insieme a una descrizione dei dati **finanziarie.**

necessari per completare la loro

attestazione quali “nome”,

“IBAN” e “indirizzo”.

L’utente allega quindi le informazioni di identità cifrate per

ogni attestazione di identità, utilizzando la chiave pubblica

del destinatario. Gli accreditatori valutano le informazioni

restituite loro dall’utente e lo rendono pubblico sulla

Blockchain se hanno soddisfatto le loro richieste.

Esempio di attestazioni di identità

• **Verifica dell'identità elettronica:** verifica di dati

aziendali

di identità mediante control i incrociati forniti da una

moltitudine di registri privati e pubblici provenienti da tutto

Esistono molti tipi di attestati di identità che possono il mondo.

essere supportati da CommercioID. Di

seguito è riportato

un elenco non esaustivo dei potenziali tipi di attestato.

• **Verifica documentale:** verifica di un documento

d'identità come il passaporto o la patente di guida e del a

corrispondenza tra l'immagine del a persona sul documento

e l'utente.

• **Verifica sociale:** verifica del e informazioni sul 'identità

degli utenti tramite i social network come Facebook e

analisi del grafico dei loro amici per contribuire a ridurre le

frodi.

• **Verifica screening:** assicurarsi che un utente non sia su

uno dei molti programmi di sanzioni globali gestiti da vari

governi in tutto il mondo.

• **Persone politicamente esposte:** assicurarsi che un

utente non sia considerato una persona politicamente

esposta (una persona con una funzione politica prominente

che è ad alto rischio di potenziale corruzione).

La verifica del a mail è altrettanto semplice perché basta

cliccare un link di un messaggio di conferma ricevuto

Il mondo del ’identità decentralizzata è maturato, sono nati i dal ’utente.

primi standard industriali:

Un account di Commercio.network completo avrà

- **Decentralized Identifier Spec.**

potenzialmente quindi un doppio fattore di autenticazione

(2FA) (telefono e mail). Una volta fornito il numero di telefono

- **Decentralized Identity Foundation.**

o la mail, creare una nuova identità è

facile come creare un

• **W3C Verifiable Claims Working Group**[5].

account su Ethereum.

Il vantaggio più evidente per gli utenti è che ora è molto

più facile creare un'identità e l'obbiettivo primario di

Commercio.network è di creare una nuova identità in meno

di un minuto. Possiamo generare un'identità creando un

account di Commercio.network. Per creare un account su

Commercio.network servono due credenziali: telefono e

Login

email. Inizialmente ad un utente viene chiesta una del e due,

per limitare al massimo la difficoltà di adozione. Se un utente

scarica l’App mobile verrà richiesto prima il cel ulare, più

avanti la mail. Al contrario, se un cliente si registra da web

verrà richiesta prima la mail e successivamente il cel ulare.

La verifica dei numeri di telefono è un processo abbastanza

semplice perché la prima volta che usa l'App l'utente deve

inserire un PIN di 6 cifre che si riceve tramite SMS.

5 https://w3c-ccg.github.io/did-spec/

Identità diversa da account

Abbiamo compreso che su

Commercio.network distinguiamo tra un' identità e un

account. Un account rappresenta la vostra utenza al 'interno del sistema, mentre

un' identità rappresenta l'alter ego che utilizzerete durante la comunicazione con un

particolare utente.

Un indirizzo di identità segue lo standard DID (Distributed Identifier) ed è preceduto

dal prefisso did. In particolare, i DID di Commercio.network saranno preceduti

dal

prefisso ***did:comnet***, ad esempio:

did:comnet13rn5cv0pjp0rgcjjj53zjcks45

Tutti gli account Commercio.network vengono creati sul a Mainnet. Che cosa

significa “creato”?

Poiché la creazione di un account corrisponde al a creazione di un account

Blockchain, non è necessario eseguire una transazione spendendo molto GAS.

D’altra parte, condividere un’ identità significa utilizzare il registro di identità

di

Commercio.network distribuito sul a blockchain per registrare eventuali modifiche

al a proprietà del e chiavi in futuro. Quindi la verifica del e firme avviene cercando la

chiave di cifratura autorizzata sul a blockchain stessa.

Commercio.network in sostanza genera sempre due nuove

identità DID (Pairwise) per ogni coppia

di aziende/utenti che

interagisce sul nostro network , con lo scopo di aumentare

significativamente la privacy degli utenti. Un proprietario di

identità pubblica, in questo caso, è in grado di control are più

identità private (a seconda del e diverse relazioni stabilite

con altre entità). Inoltre, c'è anche l'altro possibile caso d'uso

in cui un proprietario di identità potrebbe utilizzare un unico

DID per stabilire un “volto” rispetto ad un contesto specifico

(per esempio un “aspetto finanziario” per interagire con le

Massima privacy on-chain

banche). Quindi, quali sono le differenze tra questi due “tipi”

di DID e come vengono definiti i DID pubblici rispetto ai DID

Per la maggior parte degli utenti non tecnici l’idea che tutte le privati a coppie (Pairwise)? Nessuno dovrebbe capire lo

transazioni sul a Blockchain siano pubbliche è molto difficile scopo dei DID di un altro proprietario di identità, a meno che

da capire. È abbastanza destabilizzante che, su Ethereum, la correlazione non riveli loro tali informazioni. Pertanto, i

utilizzado lo stesso indirizzo per più app, sia molto facile due model i di utilizzo del DID sono indistinguibili per quanto

rivelare inavvertitamente il proprio patrimonio di Token riguarda il nostro registro. Nei contesti di un agent, un DID

posseduti mentre si sta acquistando un

CriptoKitty, durante privato e uno pubblico sembrano identici e sono gestiti al o

una partita su VirtuePoker o si fanno offerte per un concerto stesso modo per quanto riguarda il consumatore di un DID,

su GitCoin.

ma se vogliamo che il nostro agent esponga ad altri un DID

Commercio.network genera:

pubblico contro un DID privato, dovremmo poter configurare

l’agent per seguire i nostri desideri.
Così il luogo principale

• **Una singola identità pubblica divulgabile a chiunque** dove si potrebbe vedere una differenza è nel e istruzioni che

(tramite ad esempio un QR sul sito Web).

diamo al nostro agent.

• **Un numero di identità private pari al numero di relazioni Gli individui che vogliono mantenere la privacy non**

con altre aziende.

devono utilizzare lo stesso DID in più di una relazione.

115

Tutti i DID sono sul registro e sono visibili pubblicamente.

CommercioID API consente di eseguire importanti

Ma i dati allegati al DID, memorizzati nel DID Document, **operazioni di identità. Queste tre funzioni di base sono:**

possono contenere tutti i tipi di informazioni. Il proprietario

del DID potrebbe desiderare di pubblicare nel DID Document **Manage:** il sistema permette di creare un DID pubblico, oltre

alcune informazioni che possono essere pubbliche.

che gestire i contenuti nel suo DID Document.

Ad esempio, un negozio può pubblicare alcune informazioni **Connect:** il sistema permette di generare un DID a coppie

sul a sua posizione, orari di apertura, nome, ecc.

tra due entità che vogliono connettersi

sfruttando i rispettivi

Un individuo può semplicemente mantenere il DID Document DID pubblici attraverso un invito o un'interazione fisica.

senza altre informazioni oltre al a chiave di verifica e

al 'endpoint. Tutte le informazioni che inserite su un DID **Delegate:** il sistema permette di aggiungere tempo-

Document possono essere viste da tutti. Quindi, se alcune raneamente un delegato firmatario al vostro DID. Questo è

informazioni sono private, non vanno messe sul registro. un DID che può firmare un oggetto per voi.

CommercioID è una REST API che dà agli utenti, in possesso

di membership valida, l'accesso al nostro sistema di

identità decentralizzata (DID) sulla Blockchain senza

possedere alcuna esperienza di Smart Contract.

Le applicazioni scritte in una varietà di linguaggi di

programmazione potranno integrarsi in modo semplice

attraverso le nostre API. Questo insieme di funzioni dovrebbe

consentire l’esecuzione del a maggior parte dei casi d’uso

del e applicazioni, con ulteriori aggiunte in futuro.

Connessione fra aziende

non la conoscenza stessa. In caso contrario, la dichiarazione

non sarebbe provata a conoscenza zero perché fornisce al

Uno dei problemi fondamentali della Blockchain è che verificatore informazioni aggiuntive sul a dichiarazione nel

tutte le sue transazioni sono pubbliche, e le aziende nella protocol o stesso. Una prova di ZK del a conoscenza è un

maggior parte dei casi hanno la necessità strategica caso speciale quando la dichiarazione consiste solo nel fatto

di non rivelare determinate informazioni sui propri che il prover possiede le informazioni segrete.

clienti e fornitori per non offrire un vantaggio ai propri

concorrenti.

Su CommercioID di Commercio.network è in fase di studio

un sistema ZK per permettere al e aziende di creare una

È possibile utilizzare una tecnologia criptografica connessione e scambiarsi documenti in modo completamente

abbastanza esotica chiamata Zero Knowledge (ZK). privato ed anonimo, ma contemporaneamente di poter

Nella criptografia, una prova a conoscenza zero o un provare a farlo senza dover rivelare il contenuto del docu-

protocollo a conoscenza zero, è un metodo con il quale mento.

una parte (il prover), può dimostrare ad un'altra parte (il

verificatore) di conoscere un valore x, senza trasmettere

alcuna informazione riguardante
come tale valore è noto

L'essenza delle prove a conoscenza
zero è che è banale

provare che si possiede la conoscenza
di certe informazioni

semplicemente rivelandole; la sfida è
provare tale

possesso senza rivelare le
informazioni stesse o qualsiasi

informazione aggiuntiva.

Se la prova di una dichiarazione
richiede che il prover possieda

informazioni segrete, al ora il verificatore non sarà in grado

di provare la dichiarazione a nessun altro senza possedere le

informazioni segrete. La dichiarazione che viene provata deve

includere l'affermazione che il prover ha tale conoscenza, ma 117

Processo di Autenticazione Strong

In breve, la SCA è un processo di autenticazione che

deve includere almeno due dei tre tipi di fattori di

Chiaramente un sistema che dà accesso a tutte le identità
autenticazione:

deve avere un adeguato livello di autenticazione, per

dimostrare in ogni momento che, chi sta eseguendo • **Conoscenza:** qualcosa che solo il cliente conosce (ad

le operazioni consentite utilizzando CommercioID, sia esempio, password o PIN).

effettivamente la persona titolare dell'identità.

• **Possesso:** qualcosa che solo il cliente possiede (ad

Esiste una nuova direttiva pagamenti in ambito bancario esempio la carta, il generatore di codice di autenticazione,

PSD2 chiamata Strong Customer Authentication (SCA). l'identity Token).

È indirizzata esclusivamente ai TTP (Trusted Third Party • **Inerenza:** definito anche Dynamic Linking, ovvero

Player), che si articolano in AISP (Account Information l'evidenza che l'utente intenda espressamente autorizzare

Service Provider) e PISP (Payment Initiator Service Provider), una specifica transazione tramite un’associazione univoca

sebbene fuori dal o SCOPE di Commercio.network, essa può del processo di autenticazione con il contenuto del dato da

essere utile come punto di riferimento poiché non è escluso autenticare/sottoscrivere.

che l’ECOM Token, che è la moneta che servirà per eseguire

le transazioni sul a Blockchain di Commercio.network, possa

essere usato come criptomoneta effettiva.

I clienti ovviamente danno priorità al a semplicità d’uso

La PSD2 introduce requisiti di sicurezza più severi per l’avvio rispetto al a sicurezza, ma la situazione sta lentamente

e l’elaborazione del e operazioni di pagamento elettronico cambiando con l’aumento del a sicurezza obbligatoria

e per l’accesso ai conti. In un documento tecnico del a introdotta dal e autorità di regolamentazione.

PSD2 vengono il ustrate in dettaglio la Strong Customer L’avvio di un’autenticazione a due fattori per ogni

Authentication (SCA) e le regole relative a quando e come transazione o accesso al ’account ha un impatto significativo

un Payment Service Provider (PSP) debba garantire sul ’esperienza del cliente.

l’autenticazione di un cliente che richiede di effettuare un

pagamento o di gestire il proprio account.

Le situazioni in cui un PSP non è obbligato ad utilizzare SCA La PSD2 pone le basi per un'autenticazione del e operazioni

comprendono il momento in cui il cliente si trova a:

di pagamento basata sul rischio, contribuendo così in modo

determinante a ridurre l'attrito del a clientela.

- **Effettuare un pagamento senza contatto presso il**

punto vendita.

CommercioAUTH è una componente fondamentale del a

piattaforma di Commercio.network che aiuta a stabilire, con

• Accedere nuovamente ai dati del proprio conto di

quasi assoluta certezza ed in ogni momento, che chi sta

pagamento (entro i termini stabiliti).

eseguendo le operazioni consentite nel nostro network, sia

• **Pagamento per trasporto e/o parcheggio.**

effettivamente la persona titolare del ’identità CommercioID.

• **Effettuare un pagamento di basso valore.**

In genere i siti web e le applicazioni utilizzano gli

indirizzi e-mail come identificatori digitali per eseguire

• **Pagare un “beneficiario fidato”.**

l’autenticazione e l’accesso al e applicazioni. Queste sono

• **Effettuare un’operazione ricorrente per lo stesso**

accoppiate con password o con Token OAuth2/OIDC per

importo.

convalidare la proprietà. Questo crea molti problemi tra cui

la gestione del e password (un male per gli utenti e per gli

• **Spostare denaro su un altro conto o conti presso lo**

sviluppatori, un bene per gli hacker) e la necessità di affidarsi

stesso PSP.

ad un server di autenticazione di terze parti.

• Effettuare un pagamento a distanza a basso rischio

CommercioAUTH è un sistema “Passwordless” per eliminare

tramite un PSP con bassi livelli di frode.

e-mail e password e fornire un’opzione di autenticazione più

Evidentemente queste clausole corrispondono a regole fisse elegante,

più sicura e più semplice.

di uso limitato o a parti autenticate in precedenza. Tuttavia, Ogni singolo utente di Commercio.network dovrà scaricare

l’ultimo caso fornisce ai PSP un certo livel o di control o sul e l’App e generare una CommercioID Keystore. Questa funzione

transazioni, a condizione che effettuino un’analisi del rischio del a Blockchain potrebbe essere usata come base per un

di transazione.

sistema di autenticazione per i siti web e

per le App.

119

CommercioAUTH permette agli utenti di autenticarsi sui

siti web e sulle applicazioni senza fare affidamento sulle

password o su un'azienda centralizzata come Google,

Twitter o Facebook.

La differenza di CommercioAUTH è che:

• Gli utenti potrebbero invece utilizzare

un Blockchain wal et

keystore che già control ano.

• Gli utenti potrebbero utilizzare un plugin, un’App oppure

un qualsiasi browser web3 abilitato per potersi autenticare

senza login e password.

I principali vantaggi di questo rivoluzionario sistema

sono i seguenti:

• Non è necessario memorizzare localmente le password

degli utenti, ma solo le sessioni.

• Non è necessario includere le funzioni di “reimpostazione

password” (forgot password).

• Non è necessario memorizzare le chiavi API per i servizi

OAuth.

• Non c’è alcuna dipendenza da un’azienda esterna le cui API

potrebbero non funzionare in qualsiasi momento, bloccando

l’applicazione.

La fine delle password?

dovrebbe mai essere rivelata in nessuna circostanza.

Le password rappresentano una delle principali falle CommercioAUTH è una REST API che dà agli utenti in

di sicurezza del web moderno. La maggior parte degli possesso di autenticazione valida l'accesso al nostro sistema

sviluppatori di siti web ad oggi non implementano sul a Blockchain senza dover avere alcuna esperienza di

correttamente la memorizzazione delle password, cioè Smart Contract.

non fanno un SALT hash o addirittura NON criptografano Le applicazioni scritte in una varietà di linguaggi di

le password, Tutto ciò lascia agli hacker un tesoro di programmazione potranno integrarsi in modo semplice

password plaintext (leggibili) da trovare: le cronache dei attraverso le nostre API. Questo insieme di funzioni dovrebbe

DATA BREACH riempiono le pagine dei giornali.

consentire l’esecuzione del a maggior parte dei casi d’uso

Utilizzando le autorità centrali per OAuth, gli utenti danno del e applicazioni, con ulteriori aggiunte in futuro.

il proprio consenso a sacrificare tutti i diritti di privacy e di **Che cosa puoi fare con l’API di CommercioAUTH?**

utilizzo a tali autorità. La proposta CommercioAUTH intende

risolvere questo problema in modo completamente CommercioAUTH API consente di eseguire importanti

decentralizzato e cambiare le regole del gioco per sempre.

operazioni di autenticazione. Queste due funzioni di base

sono:

Una soluzione decentralizzata consentirebbe al ’utente di

mantenere il control o dei propri dati (a quali siti ha effettuato **REGISTER:** il sistema consente al ’utente di ricevere un invito

l’accesso) senza far sapere a Facebook, a Google o a chiunque da un membro del a rete e di registrarsi nel sistema.

altro le proprie attività (GDPR privacy by design). Inoltre **LOGIN:** il sistema consente al ’utente di accedere a un

questa soluzione non richiederebbe di dover mantenere un sistema senza l’uso di una password.

nodo attivo e sincronizzato del a Blockchain e tale metodo

utilizzerebbe solo la matematica ECDSA (El iptic Curve Digital

Signature Algorithm) offline per validare che il client control i

la chiave privata di un dato indirizzo Blockchain pubblico.

La chiave privata non verrebbe mai rivelata dal client e non 121

Processo di Firma decentralizzato

•**Firma Elettronica semplice:** sono comprese tutte le forme

di firma digitalizzata, un'immagine al egata di una firma o il

Nel luglio 2016 è entrato in vigore nel 'UE il sistema eIDAS clic su un pulsante "Accetto".

di eSignature. Questa legislazione garantisce che tutti i suoi

Stati membri non possono respingere le

firme elettroniche •**Firma Elettronica Avanzata (FEA):** una firma che solo

solo perché non sono fatte su carta. Inoltre, fornisce agli la parte firmataria può creare. Inoltre la firma è col egata

Stati membri gli strumenti per attribuire effetti giuridici al a ai dati in modo che, se i dati cambiano in seguito, la firma

firma elettronica. Concretamente, eIDAS definisce tre livel i viene invalidata. eIDAS e il DPCM del 2014 [6] hanno la

di firme elettroniche, ciascuno dei quali è caratterizzato da necessità di identificare in modo certo il firmatario

al ’atto

un livel o più elevato di verifica del ’identità del firmatario, del ’attivazione del a firma.

sicurezza e non disconoscibilità.

•**Firma Elettronica Qualificata (FEQ):** una firma elettronica

avanzata creata utilizzando un certificato qualificato e

supportata da un fornitore di servizi fiduciari (Trust Service

Provider - TSP). eIDAS e il DPCM del 2014 hanno la necessità di

identificare in modo certo il firmatario al ’atto del ’enrol ment

del a firma.

6 DPCM 13 novembre 2014 (si veda: https://www.agid.gov.it/sites/de-

fault/files/repository_files/regole_tecnic
)

122

A tutt’oggi non esiste una legislazione UE che imponga qualificate. Le Blockchain Pubbliche consentono a chiunque

quando un firmatario debba utilizzare un

certo livel o di di approvare una transazione indipendentemente da chi,

firma elettronica: eIDAS lascia agli Stati membri la libertà dove e come viene creata la firma. L'autore di una Firma

di stabilire i propri requisiti di firma per una transazione. Qualificata ha bisogno del 'approvazione di un QTSP, il che

L'unico tipo di firma universalmente riconosciuto da tutti gli significa essere identificato, control ato e attuare una serie

Stati membri del 'UE è la Firma Qualificata, che equivale a di politiche

rigorose.

una firma manoscritta davanti al notaio.

Commercio.network ha creato un processo di firma

elettronica semplice di documenti commerciali

decentralizzato, distribuito e non disconoscibile,

basato sulla tecnologia della Blockchain chiamato

CommercioSIGN.

Per garantire uno status giuridicamente

vincolante al ’interno

del ’UE, le transazioni dovrebbero essere firmate con firme

qualificate. eIDAS è stato concepito per essere agnostico dal

punto di vista tecnologico. Una firma su Blockchain potrebbe

soddisfare i criteri stabiliti per le firme elettroniche avanzate,

solo a condizione che sia avvenuta l’identificazione del

soggetto titolare del e chiavi di firma, cosa che accade

raramente.

Esiste quindi uno squilibrio fondamentale tra le firme

apposte su Blockchain Pubbliche e quel e apposte con firme

123

Firme avanzate e legislazione locale

Questi tre requisiti si completano a vicenda in modo da

fornire, nel loro insieme, una ragionevole garanzia del a

Invece di cercare un’accettazione su

scala europea di una qualità di una firma. Tuttavia, non tutte sono sufficientemente

firma elettronica, possiamo considerare i requisiti dei singoli specifiche per essere direttamente applicabili. In caso di

Stati nazionali per la firma elettronica. Ad esempio, nei Paesi conflitto, la valutazione di questi aspetti richiede un'analisi

Bassi l'articolo 3:15a del codice civile olandese (DCC) tratta del e circostanze specifiche in cui un documento è stato

degli effetti giuridici del e firme

elettroniche.

firmato.

Esso stabilisce che una firma elettronica deve soddisfare tre Va escluso che CommercioSIGN possa mai essere considerata

criteri per essere giuridicamente equivalente ad una firma una Firma Qualificata per i limiti entro cui questa è stata

manoscritta:

definita, in particolare a causa del a necessità di utilizzare un

profilo emesso da un ente certificatore nazionale o europeo.

• **La firma deve soddisfare i criteri eIDAS per una firma**

Per poter diventare un atto giuridicamente vincolante

elettronica semplice o avanzata.

universalmente accettato nel ’UE, un’operazione sul a

Blockchain dovrebbe essere firmata con una Firma Qualificata.

Sebbene tecnicamente possibile, non è praticamente

auspicabile avere firme qualificate su un registro pubblico

• **La firma elettronica deve svolgere le stesse funzioni di**

senza autorizzazione. Al contrario, la legislazione locale

base di una firma manoscritta.

sul e firme elettroniche può essere sfruttata per ottenere gli

stessi effetti giuridici da qualsiasi firma elettronica. In caso di

conflitto, le circostanze del a firma determinano se l’accordo

• Il metodo utilizzato per la firma deve essere

è giuridicamente vincolante.

sufficientemente affidabile in considerazione dello

scopo dell'accordo.

124

Le firme elettroniche sono in circolazione da un po' di tempo Nel a maggior parte dei casi la firma elettronica è

e stanno diventando sempre più popolari grazie al a spinta memorizzata al

’interno del documento. Questo significa

verso la Digital Transformation in corso nel a maggior parte che chiunque abbia bisogno di control are se un documento

del e aziende e dei paesi. È chiaro che stampare su carta e è firmato, avrà anche pieno accesso in lettura a tutti i

firmare i documenti per poi doverli riscansionare non è un contenuti del documento.

esempio di Digital Transformation per un’azienda.

Questo non è il massimo per certi documenti riservati!

Ci sono varie ottime soluzioni di firma elettronica disponibili

oggi sul mercato. Queste soluzioni hanno molteplici

funzionalità, ma di fatto consentono di aggiungere firme

legalmente vincolanti ai documenti. Offrono inoltre la

possibilità di far firmare i documenti a terzi utilizzando due

standard:

- **PAdES: e-firma per documenti PDF.**

• XAdES: e-firma per documenti XML.

125

La Firma Elettronica con chiavi

asimmetriche

La firma elettronica dal punto di vista tecnico è uno schema

matematico per la rappresentazione dell'autenticità di

messaggi o documenti digitali. Una firma elettronica valida

dà al destinatario la ragione di

credere che:

• Il messaggio sia stato creato da un mittente dichiarato.

(Paternità del messaggio).

• Il mittente non possa negare di aver inviato il

Le chiavi sono semplicemente grandi numeri che sono stati

Paternità Non ripudiabilità Integrità

messaggio. (Non ripudiabilità).

accoppiati ma che non sono identici (asimmetrici).

Una chiave del a coppia può essere condivisa con tutti; si

• Il messaggio non sia stato alterato durante il

chiama chiave pubblica. L'altra chiave del a coppia è tenuta

trasporto. (Integrità).

segreta; si chiama chiave privata.

Le firme elettroniche sono spesso utilizzate per applicare Entrambe le chiavi possono essere utilizzate per criptare un

le firme tramite un computer, un termine

più ampio che messaggio: la chiave opposta a quel a utilizzata per criptare

si riferisce a tutti i dati elettronici che hanno lo scopo di il messaggio è utilizzata per la decrittazione, che in molti casi

una firma. D'altra parte non tutte le firme elettroniche fornisce un livel o di convalida e sicurezza ai messaggi inviati

utilizzano le firme digitali. Le firme elettroniche utilizzano attraverso un canale non sicuro.

la criptografia asimmetrica, nota anche come criptografia a ***Le firme elettroniche sono per molti versi***

equivalenti

chiave pubblica (PKI), che utilizza chiavi pubbliche e private ***alle tradizionali firme manoscritte, ma una loro corretta***

per criptare e decodificare i dati.

applicazione è più difficile da falsificare rispetto ad uno

scarabocchio su un pezzo di carta.

Multisignature

La Multisignature (multifirma) è uno

schema di firma digitale La firma multipla (spesso chiamata Multisig) è una forma di

che consente a un gruppo di utenti di firmare un unico tecnologia utilizzata per aggiungere ulteriore sicurezza per

documento. Di solito, un algoritmo di firma multipla produce le transazioni in Criptovalute. Gli indirizzi Multisig richiedono

una firma congiunta che è più compatta di una raccolta di che un altro utente o più utenti, firmino una transazione di

firme distinte di tutti gli utenti.

denaro, prima che possa essere trasmessa nel a Blockchain.

La firma multipla può essere considerata una Il numero richiesto di firme viene concordato all'inizio

generalizzazione sia della firma di gruppo che della firma quando le persone accettano di creare l'indirizzo.

ad anello.

La firma multipla permette la creazione di due su tre servizi

di escrow (acconto di garanzia).

Ad esempio: quando Alice vuole pagare Bob, invia ***Nonostante il nome, la firma multipla su una Blockchain***

una transazione ad un indirizzo Multisig, che richiede ***è solo un elemento riassuntivo di una relazione di firme di***

almeno due firme del gruppo per riscattare il denaro. ***utenti distinti, non una singola entità.***

Se Alice e Bob non fossero d'accordo su chi deve ricevere ***Lo schema di firma multipla è implementato anche***

in

il denaro (Alice vuole un rimborso, mentre Bob chiede *diverse valute criptografiche.*

il pagamento), possono rivolgersi ad un terzo: Charlie.

Charlie può porre a sua scelta la sua firma ad Alice o Bob,

in modo che solo uno dei due possa riscattare i fondi.

Alice

Bob

Charlie

128

129

06

Capitolo Sesto

la Governance aziendale con la Blockchain

Dai consigli di amministrazione al e DAO

FARE **Business** CON LA **Blockchain**

Capitolo Sesto

La Governance

aziendale con la

Non chiediamo ai comuni cittadini non addestrati di

eseguire interventi chirurgici, far volare un aereo, progettare

Blockchain

computer o svolgere gli altri innumerevoli compiti necessari

per mantenere la società in funzione.Cosa rende diversa la

Governance?

Dai consigli di

amministrazione al e DAO

Il problema è semplice: se diamo la Governance agli “esperti”,

essi prenderanno decisioni nel loro stesso interesse, non nel

migliore interesse di tutti noi. Come abbiamo visto troppo

Le democrazie sono comunità che chiedono ai propri membri spesso in passato, questo porta al ’arricchimento di una

tramite voto di prendere del e decisioni

di governo: chi deve piccola élite.

guidare, quali politiche seguire, quali leggi emanare. In tutte Possiamo sfruttare l'esperienza dei migliori e più bril anti,

queste domande le democrazie invitano i comuni cittadini isolando il sistema dai tentativi che potrebbero fare per

a prendere decisioni complesse con conseguenze spesso ottenere il control o?

movimentate.

La ricerca moderna sulla "saggezza delle folle" fornisce

nuove intuizioni su come combinare le competenze di

tutti i partecipanti senza cedere il controllo agli "esperti".

In combinazione con la ricerca sul e organizzazioni autonome

decentrate (DAO), questo ci permette di progettare una

nuova forma di democrazia più stabile, meno incline a

comportamenti errati, in grado di soddisfare le esigenze dei

suoi cittadini e che utilizza meglio

l’esperienza di tutti i suoi

cittadini per prendere decisioni di alta qualità.

132

DAO

133

La nascita di una nuova persona

giuridica: la DAO

Che cos’è una DAO? L’acronimo sta per Organizzazione

Autonoma Decentrata. Il concetto di

DAO deriva da

Bitcoin, che potrebbe essere visto come il primo prototipo

di DAO, e da Ethereum dove esistono vari esempi di DAO.

In breve, Bitcoin è il primo esempio di una nuova forma di

vita.

Vive e respira su internet.

Vive perché può pagare le persone per mantenerlo in vita.

Vive perché svolge un servizio utile

che le persone pagano

per essere svolto.

Vive perché chiunque, ovunque, può eseguire una copia del

suo codice.

Vive perché tutte le copie in esecuzione sono costantemente

in dialogo tra loro.

Vive perché se una copia è corrotta viene scartata

velocemente e senza nessuna confusione.

Vive perché è radicalmente trasparente: chiunque può

vedere il suo codice e osservare esattamente cosa fa.

Non può essere cambiato.

Non si può discutere.

Non può essere manomesso.

Non può essere corrotto.

Non può essere fermato.

Non può nemmeno essere interrotto: se

la guerra nucleare

distruggesse metà del nostro pianeta, esso continuerebbe

a vivere, senza corruzione. Continuerebbe a offrire i suoi

servizi e a pagare le persone per mantenerlo in vita.

L'unico modo per spegnerlo è uccidere ogni server che lo

ospita. Il che è difficile, perché molti server lo ospitano, in

molti paesi, e molte persone vogliono usarlo.

Realisticamente, l’unico modo per ucciderlo è rendere il

servizio che offre così inutile e obsoleto che nessuno voglia

usarlo. Così obsoleto che nessuno voglia pagarloe nessuno

voglia ospitarlo. Al ora non avrà più soldi da pagare a

nessuno. Morirà di fame.

Ma finché ci sono persone che vogliono usarlo, è molto

difficile da uccidere, da corrompere o da interrompere.

La comunità tecnica è stata affascinata da questa nuova **Si potrebbe creare un'azienda cambiovalute, o di nomi**

forma di vita. Non per quel o che poteva fare, o aveva fatto, **di dominio, o un mercato di previsioni, o una fondazione,**

ma proprio perché era una nuova forma di vita.

tutte completamente autonome (e che posseggono se

stesse.9)

Chiunque voglia creare la propria nuova forma di vita digitale

su Ethereum può farlo utilizzando un progetto chiamato Il concetto di una Distributed Autonomous Organization/

Aragon.one.

Corporation (DAO/DAC) è il risultato ideale del a rivoluzione

criptotecnica. Le sue radici affondano in temi sul

Aragon ti permette di organizzarti e collaborare decentramento organizzativo che sono stati descritti da Ori

liberamente senza confini o intermediari.

Brafman in The Starfish and the Spider (2007)[7] e quel i sul a

Crea organizzazioni, aziende e comunità globali e senza “peer production”, giustamente descritti da Yochai Benkler

burocrazia.

in The Wealth of Networks (2006)[8]. Ma questi due temi sono

stati recentemente affiancati dal ’avvento del e tecnologie

Come Bitcoin, la tua DAO vivrà su internet. Come Bitcoin, legate al a crittocorrente da Dan Larimer, che ha osservato

sopravviverà finché farà qualcosa per cui la gente pagherà. che Bitcoin è il DAC originale, e da Vitalik Buterin, che ha

Come Bitcoin, non ci sarà modo di ucciderla. Come Bitcoin, ampliato questo costrutto generalizzandolo ulteriormente

sarà radicalmente trasparente. Come Bitcoin, non potrà come DAO, notando che il DAO ha “capitale interno”.

essere fermata. Come Bitcoin, sarà in grado di pagare le

persone per fare tutto ciò che la gente è disposta a fare in

cambio del a sua criptovaluta. A differenza di Bitcoin, seguirà

le proprie regole, qualunque sia il modo in cui sono state 7 Brafman, O. , & Beckstrom, R. (2007), ***The starfish and the spider: the***

programmate quando è stata creata.

unstoppable power of leaderless organizations, London Portfolio/Pen-

guin.

8 Benkler, Y. (2006), ***The wealth of networks: how social production***

transforms markets and freedom, New Haven Yale University Press.

DAO

La deregolamentazione del crowdfunding e del a

disaggregazione dei servizi erano due temi accoppiati, e

il tutto era turbocompresso da un livel o di Governance

criptotecnica di tecnologie e automazioni basate sul a

fiducia per consentire al e DAO di ***"funzionare senza alcun***

coinvolgimento umano sotto il controllo di un insieme

incorruttibile di regole di business" .

Quindi, come ci si arriva e quali sono i pezzi del puzzle da un

Se la DAO è la massima espressione in termini di

punto di vista operativo/pratico?

autonomia aziendale, allora potremmo immaginare

Solo perché possiamo andare su **https://aragon.org** e creare

un percorso a sei passi verso una sequenza evolutiva,

una DAO in cinque minuti, questo non significa che la DAO

dove ogni stadio successivo si basa sulle funzioni del

avrà successo.

precedente, secondo la seguente evoluzione:

Anche se è possibile partire con una DAO fin dal primo giorno

di pianificazione di un'iniziativa, è anche possibile evolvere

verso di essa, ed è ugualmente possibile incorporare parti di

un costrutto DAO in un'organizzazione tradizionale.

Fase Partecipativa: gli utenti partecipano

volontariamente e autonomamente a compiti non

impegnativi.

Fase Collaborativa: gli utenti col aborano e hanno

un valore aggiunto verso scopi o obiettivi comuni.

Fase Cooperativa: gli utenti si aspettano che

alcuni guadagni condivisi vengano restituiti.

Fase Distributiva: viene avviata la propagazione

di queste funzioni moltiplicandole su una rete più

ampia.

Fase Decentralizzata: un'ulteriore scalabilità viene

raggiunta infondendo più potenza ai bordi.

Fase Autonoma: agenti autonomi, programmi

intel igenti e (più tardi) aumentati livel i di

intel igenza artificiale e algoritmi di A.I.

forniscono auto-sostenibilità nel e operazioni e

creazione di valore nei centri, bordi e arteri di

un’organizzazione.

9

A.I.: Artificial Intelligence

139

Checklist di implementazione di una DAO

Ci sono vari componenti su cui bisogna pensare in modo

metodico. Ecco una checklist di implementazione da

affrontare gradualmente:

Quale ambito di applicazione? Gli utenti sono al centro di

questa evoluzione, così come l’architettura per supportare

queste azioni degli utenti. Si noti che le funzioni partecipative,

col aborative e cooperative sono basate sul ’utente, mentre

quel e distribuite, decentralizzate e autonome sono basate

sul ’architettura.

Tipi di proprietà: ci sono tre modi per essere coinvolti in una

DAO: puoi comprare azioni, Criptovaluta o Token; possono

essere concessi a te; oppure puoi guadagnarli. La parte di

guadagno è interessante perché comporta un lavoro attivo

o passivo. Un esempio d

Ti i la

pi voro

di a ttivo include la consegna

Unità di

Trasparenza

di bounties per progetti specifici come la ricerca di bug, lo

proprietà

valore

nella Governance

sviluppo di software, l'hacking etico o qualsiasi altro compito

richiesto dal a DAO. Il lavoro passivo

si ottiene tipicamente

condividendo qualcosa, come i cicli di elaborazione del

computer, l'accesso a Internet, lo spazio di archiviazione o

anche i dati.

140

Guadagnare

C i

Unità di valore: ciò che si riceve in cambio del a posta in **Trasparenza nella Governance:** ottenere una

Governance

gioco può anche assumere molte forme. Naturalmente, il corretta non è facile, ma tale obiettivo deve essere perseguito.

tradizionale strumento è un'azione (o una obbligazione), ma L'autonomia non implica anarchia, quindi è necessario

il valore può anche arrivare in punti, Token, ricompense o pensare al e varie parti che compongono la Governance, sia

Tipi di

Criptovalute. Si noti che i Toke

Un n ***i*** p ***t*** os ***à*** sono

di a vere scopi multipli, che gli stakeholder s

T ia ***r*** no

a c ***s*** oinvo

pa lt ***r*** i atti

en vame

za nte (ad esempio,

Tipi di

Unità di

Trasparenza

in quanto possono rappresentare diritti d'uso del prodotto o votare, gestire, creare le regole, control are le regole,

propr

pr

i

opr et

i à

et

valore

nella Governance

diritti di proprietà legati a

v d u

a n c

l er

or to valo

e re intrinseco.

prendere dec

n isio

el n ***l*** i, ***a*** rifer

G ire, r

ov ego

er lam

n en

a ti)

n , ***c*** o p

e assivamente

(ad esempio, sentirsi responsabilizzati, valutati, rispettati,

equamente compensati).
Indipendentemente da ciò, deve

prevalere la trasparenza nel a Governance.

141

Gu

G a

u da

a gn

da a

gn r

a e

r

C i

Tipi di

Tipi di

Unità

Un di

ità di

Tras

Trpa

as ren

parza

en za

propr

pr iet

opr à

ietà

valor

va e

lore

nell

na G

ell ov

a Gern

ov a

er ncae

nce

Guadagnare: in senso tradizionale, abbiamo avuto la **Criptografia:** i protocol i e le piattaforme Blockchain e

partecipazione agli utili o la partecipazione ai dividendi come di criptografia basati sul a Criptovaluta

sono solo degli

forma di ridistribuzione col ettiva degli utili. Ma in una DAO abilitatori per il meccanismo del consenso. In genere, si

questi benefici potrebbero includere il voto/diritti speciali, tratta di protocol i di consenso decentralizzato open source

o l'ottenimento di uno status speciale. In definitiva, ci deve e di protocol i di fiducia decentralizzati che consentono

essere una crescita di valore attraverso l'apprezzamento del l'inconfutabilità, la verificabilità e la veridicità di tutte le

Gua

G da

ua gn

da are

gnare

C iC i

capitale sociale, per esempio sotto forma di Criptovaluta.

transazioni e dei programmi intel igenti. Questi protocol i

possono essere di uso generale (ad esempio, Ethereum,

Bitcoin).

142

Ci sono tre componenti funzionali che dovrebbero essere

inclusi nel a piattaforma tecnologica:

• Uno strato di dati utente, con l'assunzione che i dati

Uno strato di dati

sono di proprietà dell'utente e risultano accessibili solo

utente

in una specifica forma aggregata o cieca dalla DAO.

• Smart Contract, che sono i veri e propri motori di

Smart Contract

transazione.

• Varie interfacce di programmi applicativi (API) per

Varie interfacce di

interagire con servizi a valore aggiunto o partner che

programmi applica-

sono ausiliari rispetto ad una DAO.

tivi (API)

143

L’obiettivo chiave delle DAO

?

Un obiettivo chiave di una DAO è la creazione di valore o

produzione,. Per fare in modo che ciò accada è necessario

che ci sia un collegamento specifico tra le azioni

dell'utente e gli effetti di tali azioni sul valore complessivo

dell'organizzazione, come simboleggiato dal valore della

criptomoneta che ne sta alla base.

È qui che deve avvenire la creatività imprenditoriale, e

dove saranno inventati i modelli di business.

Un uso senza legame di valore è uno spreco, e si tradurrà in

un fal imento. Molte di queste DAO saranno teoriche nel e

loro fasi iniziali. Una Criptovaluta consente al a DAO solo di

iniziare un percorso: percorrere tutta la strada richiede un

Product/Market Fit, la validazione di model i di business e Al ’inizio vengono fatte molte ipotesi e la DAO può assomi-

tanti utenti (clienti) per andare avanti e guadagnare.

gliare a un film di fantascienza, almeno fino a quando il pro-

dotto o servizio si scontra con la realtà del mercato.

È sempre il mercato che decide. La "prova del successo" sarà

la sostenibilità sul mercato, non il successo del crowdfunding

iniziale del progetto.

Nonostante le difficoltà, arrivare a realizzare una DAO è

un processo di costruzione graduale che non può essere

accelerato artificialmente.

144

145

07

Capitolo Settimo

Blockchain Product Design

Sviluppo di un progetto Blockchain

FARE **Business** CON LA **Blockchain**

Capitolo Settimo

Blockchain Product Design

Sviluppo di un progetto Blockchain

Quando le aziende definiscono delle strategie spesso fanno Questo significa trovare un problema per la cui soluzione

alcuni passi falsi. Di solito raccolgono i dati del passato e qualcuno sarebbe disposto a pagare qualcosa.

fanno previsioni sul futuro basandosi su di essi, e spesso Nel nostro caso è importante capire se il problema può essere

questi stessi dati non dicono cosa i futuri clienti si aspettano. risolto solo con la Blockchain.

In alternativa fanno delle scommesse rischiose basate

sull'istinto invece che su delle prove.

Il Blockchain Product Design è un

processo strategico

che cerca di evitare questi errori tramite una serie di

?!

metodologie applicate dalle startup alla ricerca di un

modello di business profittevole, ripetibile e scalabile.

La prima e unica regola universalmente valida è costruire

qualcosa che la gente vuole.

Per capire questo, basta rispondere a sei domande:

1. Devo registrare lo stato? (Vero) (Falso)

2. Ci sono diverse persone che devono scrivere dati? (Vero) (Falso)

3. NON vuoi/puoi delegare ad un singolo soggetto terzo? (Vero) (Falso)

4. Tutte le persone che scrivono dati NON sono conosciute? (Vero) (Falso)

5. Tutte le persone che scrivono dati NON sono fidate? (Vero) (Falso)

6. È richiesta una verifica pubblica di

tutte le transazioni? (Vero) (Falso)

Se hai risposto Falso ad una di queste domande, non serve una Blockchain Pubblica,

al limite una Blockchain Federata o Privata.

Il Blockchain Product Design è un processo strategico che impiega tre metodologie

provenienti dal mondo del design innovativo, dal mondo delle startup e dal mondo

dello sviluppo software.

Il processo è diviso in tre distinte macro fasi che devono

rispondere a tre precise domande.

1) Fase Problem/Solution Fit

Ho un problema che può essere risolto con una soluzione

Blockchain?

Prima di investire mesi o anni in sforzi per la costruzione di

un prodotto Blockchain che nessuno vuole, occorre stabilire

se questo prodotto è qualcosa che valga la pena di essere

realizzato. L'unico modo per farlo è di separare il problema

dalla soluzione e tarare entrambi attraverso una serie di

3 FASI

interazioni con i potenziali clienti. Il Test del problema

consente di comprendere se si ha fra le mani un "problema

degno di essere risolto" molto prima di investire tempo,

denaro e sforzo per mettersi a costruire una soluzione. In

ambito aziendale per “problema degno” si intende che

qualcuno possa spendere soldi per vederlo risolto. Arrivati

a questo punto é possibile determinare il numero minimo

di caratteristiche che il nostro prodotto Blockchain deve

avere per risolvere il problema e passare alla prima bozza di

soluzione, creando un Proof of Concept

(POC).

150

2) Fase Prodotto/Market Fit

3) Fase Scaling

Ho costruito qualcosa che la gente vuole?

Come posso accelerare la crescita?

Appena trovato un problema degno di essere risolto e Dopo aver trovato l'incontro fra Prodotto e Mercato, ottenere

dopo aver sviluppato il Proof of

Concept, è necessario un discreto livello di successo è quasi sempre garantito.

creare un'ipotesi di modello di business basato su questo L'attenzione in questa fase finale si sposta ad accelerare le

problema/soluzione. È possibile avviare il processo di azioni di business che portano alla crescita dell'azienda

apprendimento andando dai clienti/utenti per testare quanto (scalare).

la vostra soluzione Blockchain risolva il problema. Dopo varie

interazioni con i clienti si passa progressivamente dal POC

al Minimum Viable Product (MVP). L’essenza di questa fase

consiste nella massimizzazione di tale tipo di apprendimento.

Il raggiungimento della traction (cioè trovare un incrocio fra

il prodotto e il mercato) è la prima pietra miliare significativa

per un progetto Blockchain.

Blockchain Product Design = Design Thinking + Lean Startup + Agile

Il Blockchain Product Design è un metodo che combina

tre approcci conosciuti e stimati per affrontare ognuna di

queste fasi:

• **Design Thinking:** empatizzare con gli utenti, definire

e ideare attraverso il Design Thinking.

• **Lean Startup:** trasformare le idee in modelli di

business e testare se esiste un mercato.

• **Agile:** costruire e consegnare il

prodotto in modo

incrementale e più veloce attraverso i processi Agile.

152

Questo è uno schema elaborato da Gartner che

mostra come le tre metodologie fluiscono in un

singolo percorso.

Blockchain Product Design

Nelle pagine seguenti illustriamo in estrema sintesi i

tre approcci.

153

Design Thinking (Problem/Solution fit)
Lean Startup (Product/Market fit)

Il Design Thinking è un processo iterativo in cui si cerca di Lean Startup è una metodologia per lo sviluppo di imprese

comprendere il problema dell'utente, mettere in discussione e prodotti che mira ad accorciare i cicli di sviluppo del

i presupposti e ridefinire i problemi, al fine di creare nuove prodotto e a

scoprire rapidamente se un modello di business

strategie e soluzioni basate sulla Blockchain. A differenza proposto è fattibile. Questo risultato è ottenuto adottando

del “Brainstorming”, il Design Thinking promuove il una combinazione di sperimentazione basata sull’ipotesi

“Painstorming” per comprendere appieno il “dolore” di business, rilasci di prodotti iterativi e apprendimento

dell’utente. Le fasi del Design Thinking sono le seguenti:

validato. Le fasi del Lean Startup sono le seguenti:

- **Empatizzare con gli utenti.**

- **Creare un modello di business basato sul problema e**

- **Definire le esigenze degli utenti, i loro problemi e i**

sulla soluzione Blockchain.

vostri insights.

- **Testare la soluzione e avere un feedback dai clienti.**

- **Ideare mettendo in discussione i**

presupposti e

• Passare in modo iterattivo da un POC al Blockchain.

creando delle ipotesi di soluzioni innovative.

Minimum Viable Product ascoltando il feedback dei

• Sviluppare una Blockchain Proof of Concept (POC) di

clienti.

queste soluzioni.

• Comprendere se esiste un mercato

per questo

Il Design Thinking è un approccio all'innovazione incentrato

Blockchain Minimum Viable Product trovando clienti/

sull'utente per integrare le esigenze delle persone, le

utenti paganti.

possibilità della tecnologia e i requisiti per il successo

aziendale.

Design Thinking

A livello globale, il 90% delle startup fallisce (Forbes) e

la ragione principale è il fallimento del mercato: “Fanno

prodotti che nessuno vuole”(Fortune).

La metodologia Lean Startup è nata nella Silicon Valley negli **Agile (scale)**

anni ‘90, ma l’uso della parola “lean” ha le sue radici nel

sistema di produzione snella della Toyota.

Agile è un modo scalabile di lavorare, basato sullo sviluppo

Il sistema di produzione snella di Toyota è stato usato iterativo, sulla consegna incrementale e sulla rivalutazione

per costruire le cose in modo efficiente, ma non dice cosa continua di un prodotto.

dovrebbe essere costruito.

Utilizzato principalmente nello sviluppo di software, si basa

Utilizzando le parole di Eric Ries: “Il Lean Startup fornisce un su un’idea chiara del concetto del prodotto e del

suo mercato.

approccio scientifico per creare e gestire le startup e ottenere
Contrariamente all'idea di concentrarsi su un insieme di

il prodotto desiderato nelle mani dei clienti più velocemente. caratteristiche da sviluppare, Agile si concentra prima sulle

Si tratta di un approccio di principio allo sviluppo di nuovi caratteristiche di alto valore.

prodotti".

Agile consiste nel produrre risultati

tangibili e di lavoro

dopo ogni iterazione. Secondo i dodici principi del

Manifesto Agile, "Il software di lavoro è la misura primaria

del progresso" [10].

Come nel caso di un testo da pubblicare, si tratta di

consegnare una bozza da rivedere in base ai suggerimenti

del vostro editore: non si consegna mai l'intero pezzo tutto

in una volta!

Ora andremo ad analizzare in dettaglio
le tre metodologie.

10
https://agilemanifesto.org/iso/it/manifesto

155

Design Thinking

(Problem/Solution fit)

Empatizzare: è necessario elaborare
qualche

teoria su cosa i clienti vorrebbero ma
non hanno,

Il Design Thinking, reso popolare da David M.

immergendosi nelle loro vite ed empatizzando con

Kelley e Tim Brown di IDEO e da Roger Martin

loro. Invece di fare domande su prodotti e servizi

della Rotman School, è estremamente efficace

specifici, è necessario osservare e fare domande

perché rispetto al design classico è

fortemente

sul loro comportamento.

focalizzato sul comportamento umano.

Definire le esigenze: sulla base delle risposte è

possibile a questo punto definire i problemi e le

esigenze degli utenti, e abbozzare una serie di

requisiti minimi che potrebbero costituire la nostra

soluzione.

Il Design Thinking ha quattro fasi principali:

Ideare una possibile soluzione: ideare una possi-

bile soluzione basata sulla Blockchain mettendo in

discussione i presupposti e creando delle ipotesi di

soluzioni innovative rispondendo ai requisiti mini-

mi evidenziati dagli utenti.

Testare l'idea: realizzare un prototipo di soluzione

Blockchain che sia focalizzata sulle funzioni

minime ed indispensabili che ci permettano di

effettuare una serie di test per capire come gli

utenti rispondono alla nostra soluzione.

156

157

Il Design Thinking, utilizzando un metodo di problem

solving incentrato sul comportamento

umano, permette

di sbloccare nuove opportunità e nuovi mercati.

Design Thinking

158

Brainstorm

• Prova a cercare più

User Interview

Additional

soluzioni possibili al

Test/ iterazioni

Questions

problema.

• Identifica il problema.

• Usa diverse tecniche

• Scopri chi è l’utente

• Testa i prototipi

• Descrivi le

creative.

della soluzione e chi non

con gli utenti

caratteristiche minime

lo è.

potenziali.

per il gruppo target.

Feedback

• Verifica

• Definisci il problema

l’applicabilità della

principale.

• Ricevi del feedback

tua soluzione.

dagli utenti.

Analyze customer

• Continua a sviluppare

perspective

idee.

Nuova

• Come le persone

prospettiva

percepiscono il

Prototipa

problema che hanno.

• Cè un nuovo modo in

cui puoi aiutare i clienti

• Crea un wireframe

• Esplorare il problema

a raggiungere i loro

interattivo della

da diversi punti di vista.

obbiettivi?

soluzione.

159

Blockchain Model Canvas (BMC)

Lean Startup, reso popolare da Eric Ries che ha

unificato varie discipline come il **Lean thinking** e

il **Customer development** di Steve Blank, è una

- **A. Compilare il BMC tutto in una volta:** mentre un

metodologia estremamente efficace per lo sviluppo

business plan può richiedere settimane o mesi per essere

di imprese e prodotti esso è fortemente focalizzato

scritto, il BMC dovrebbe essere disegnato tutto in una

ad accorciare i cicli di sviluppo del prodotto e a

volta.

scoprire rapidamente se un modello di business

• **B. Le sezioni possono essere lasciate vuote:** piuttosto

proposto è profittevole e ripetibile.

che cercare di trovare o discutere le risposte “giuste”,

oppure aggiungere qualcosa in fretta, è preferibile

Utilizziamo un modello a nove blocchi chiamato

lasciare vuoto e casomai tornarci in un secondo

Blockchain Model Canvas (BMC) (basato sul

momento. Alcuni elementi necessitano di più tempo per

lavoro di Ash Mayura e Alexander Ostervalder)

essere capiti. Il BMC è pensato per essere un documento

per descrivere la propria visione e un metodo

organico che si evolve nel tempo e “non lo so” da noi è

chiamato Lean Startup (basato sul lavoro di Eric

una risposta valida.

Ries per testarne la validità.

Ecco alcuni consigli prima di iniziare.

• **C. Pensa al presente:** i business plan cercano inutilmente

di prevedere il futuro: nessuno ci riesce, è impossibile.

Invece, l'idea del BMC è quel a di scrivere ipotesi sul a

base di quel o che si sa in questo momento

• **D. Utilizza un approccio incentrato sul cliente:** Si parte

dal primo blocco “Segmento clienti” e si segue un ordine

prestabilito fino al a fine.

BMC

160

Blockchain Model Canvas (BMC)

KP

KS

VP

KR

CS

la

Soluzioni

Relazione

Problemi

la Proposta

i Segmenti

KM

di Valore

CH

di Clienti

la Metrica

i Canali

C$

R$

i Costi

i Ricavi

Cos’è il Business Model Canvas?

e la facilità d’uso del Business Model Canvas, Osterwalder

Alex Osterwalder nel suo grande libro spiega un metodo abbia avuto grandissimo successo. Successivamente

fantastico per descrivere qualsiasi idea di business: il Business abbiamo creato un modello nostro chiamato BMC, più basato

Model Canvas. Con nove blocchi in una griglia disegnata con sul lavoro di Ash Mayura, che risulta veloce, conciso e in una

un pennarello su una lavagna bianca e dei post-it riesce singola pagina rappresenta tutto il modello di business di un

a spiegare qualsiasi business dell'universo. Non ci si può progetto Blockchain.

meravigliare del fatto che, per la chiarezza delle informazioni

161

KP

KS

VP

KR

CS

la

Soluzioni

Relazione

Problemi

la Proposta

i Segmenti

KM

di Valore

CH

di Clienti

la Metrica

i Canali

C$

R$

i Costi

i Ricavi

Il problema e i clienti

mente dei gruppi omogenei di clienti. Anche Facebook con

i suoi milioni di utenti ha iniziato con un segmento di utenti

Trovati questi due primi elementi, tutto il resto del BMC è più molto specifico: studenti universitari di Harvard.

semplice da completare. È per questa ragione che conviene

sempre analizzarli insieme.

Distinguere tra i clienti e gli utenti

Scrivere tre problemi principali per il segmento di clientela Se nel prodotto ci sono diversi ruoli, bisogna necessariamente

che avete in mente, descrivere i tre problemi principali che individuare i clienti. Un cliente è qualcuno disposto a

pagare

devono essere risolti.

per il prodotto. Ad esempio, in una piattaforma di blogging

Elencare le alternative esistenti.

il cliente è l'autore del blog, mentre l'utente è un lettore.

Descrivere come pensate che i vostri clienti stiano affrontando In un servizio di condivisione di foto, il cliente è il condivisore,

questi problemi oggi. A meno che non si stia risolvendo mentre gli utenti sono gli

spettatori (familiari e amici).

un problema nuovo (improbabile), la maggior parte dei Puntare il laser sui possibili primi acquirenti: i Clienti Tipo.

problemi hanno delle soluzioni esistenti. Molte volte queste Bisogna essere più specifici sul segmento di clientela e

alternative non necessariamente sono dei concorrenti.

affinare le caratteristiche minime distintive del tuo cliente

Fare l’elenco dei possibili segmenti di clienti che pensate tipo. Il tuo obiettivo è

quello di definire un primo acquirente

possano comprare il vostro servizio.

(non un cliente tradizionale).

Suddividere grandi segmenti di clienti in segmenti più piccoli

Il mito del software che risolve i problemi universali non esiste:

non si può realisticamente progettare, costruire e posizionare

un prodotto per tutti. Ci può essere l'obiettivo di costruire

un prodotto di massa, ma per iniziare è

necessario avere in

162

KP

KS

VP

KR

CS

la

Soluzioni

Relazione

Problemi

la Proposta

i Segmenti

KM

di Valore

CH

di Clienti

la Metrica

i Canali

C$

R$

i Costi

i Ricavi

La Proposta di Valore (VP)

deve contenere il perché il tuo prodotto è differente e questa

differenza deve essere rilevante.

Al centro del BMC c'è l'elemento più importante di tutto il Una buona VP dovrebbe contenere:

modello, ed incidentalmente anche il più difficile da centrare **a. Headline:** qual è

il beneficio principale offerto? In una

al primo colpo.

singola frase, si parla del prodotto e/o del cliente.

La VP deve contenere il motivo per cui il prodotto è differente **b. Sub-headline:** una spiegazione specifica di ciò che

e questa differenza deve importare. Chi visita un sito per la facciamo, per chi e perché è utile.

prima volta, vi trascorre in media otto secondi. La Proposta **c. Tre elenchi puntati:** lista dei benefici e caratteristiche

di Valore è la loro prima interazione con il prodotto. Se si crea chiave.

una VP buona, potrebbero rimanere e vedere il resto del sito.

In caso contrario, andranno su un altro sito.

Il modo migliore per trovarla è copiare dai grandi siti: ad

La buona notizia è che non occorre farlo subito al primo esempio si potrebbe visitare il sito di Square.

colpo. Come tutto sul canvas, si inizia con la migliore ipotesi

e poi in modo iterativo si migliora.

2. Crea un High Concept Pitch

Un altro esercizio utile è quello di creare un High Concept

1. Crea una Proposta di valore (VP)

Pitch, termine reso popolare da Venture Hacks nel loro e-book

La VP è un singolo e chiaro messaggio che riassume perché Pitching Hacks. Un High Concept Pitch si basa in genere su

il tuo prodotto è differente e perché qualcuno dovrebbe concetti familiari per

trasmettere rapidamente un'idea e per

spendere soldi per comprarlo. La VP è difficile da trovare diffonderla facilmente. A differenza di un VP, un High Concept

perché bisogna distillare l'essenza del prodotto in poche Pitch è utilizzato al meglio in combinazione con qualcos'altro

parole da mettere in prima pagina sul sito. Inoltre, la VP che imposta il contesto giusto, come un elevator pitch.

KP

KS

VP

KR

CS

la

Soluzioni

Relazione

Problemi

la Proposta

i Segmenti

KM

di Valore

CH

di Clienti

la Metrica

i Canali

C$

R$

i Costi

i Ricavi

La Soluzione

fra un Pivot e una ottimizzazione è che i Pivot servono per

trovare un piano che funzioni, mentre le Ottimizzazioni

Ora siete pronti per affrontare le varie ipotesi di soluzione.

accelerano tale piano.

Bisogna comprendere che, poiché tutto ciò che scriviamo sul

BMC sono solo delle ipotesi non testate, non è consigliabile

auto-convincersi di aver trovato una soluzione definitiva ai

problemi dei clienti.

In questa fase conviene semplicemente abbozzare le

caratteristiche salienti del prodotto accanto a ogni problema.

L’ideale è sforzarsi di associare una soluzione al problema

del cliente il più tardi possibile, almeno dopo averci parlato

una volta...

La Soluzione (MVP) cambierà nel tempo e, a seconda della

fase della startup in cui ci si trova, essa sarà il prodotto di

svariati Pivot ed Ottimizzazioni.

“Pivot” è un termine usato da Eric Ries per descrivere un

cambiamento di direzione di una startup durante la fase di

apprendimento. Il modo migliore per capire la differenza

KP

KS

VP

KR

CS

la

Soluzioni

Relazione

Problemi

la Proposta

i Segmenti

KM

di Valore

CH

di Clienti

la Metrica

i Canali

C$

R$

i Costi

i Ricavi

La Metrica

Ci sono solo cinque metriche chiave che guidano un progetto Blockchain:

Stage

Descrizione

Conversione

% Conversione

Valore (non costo)

Acquisition

Come gli utenti arrivano e Visitatori
App/ Landing page

60%

5 €

da che canali arrivano al tuo

(2+ pagine, 10 secondi 1+

servizio

click = non abbandonano)

Utenti entrano e si registrano

Activation

Come gli utenti si registrano

(clicks/tempo/pagine,

15%

25 €

la prima volta nel tuo

emails/registrazioni profilo,

servizio

utilizzo moduli)

Retention

Come gli utenti TORNANO al

Utenti ritornano; Visite

5%

1 €

tuo servizio più volte

Multiple

(1-3x viste/mese; Email /CTR)

Referral

Come gli utenti apprezzano Utenti invitano altri utenti

1%

5 €

il tuo servizio tanto da

(soddisfazione cliente >= 8 ;

suggerirlo ad altri

Fattore Virale K > 1)

Revenue

Come gli utenti acquistano il Utenti pagano /generano €€€

2%

50 €

tuo servizio

(break-even Target di

profitto)

165

KP

KS

VP

KR

CS

la

Soluzioni

Relazione

Problemi

la Proposta

i Segmenti

KM

di Valore

CH

di Clienti

la Metrica

i Canali

C$

R$

i Costi

i Ricavi

I Canali

INBOUND contro OUTBOUND

Come distribuire la nostra Value Proposition al cliente?

I Canali inbound utilizzano dei “messaggi pull” per consentire

Oltre a definire il prodotto giusto da costruire, è altrettanto ai clienti di trovarci organicamente, mentre i Canali Outbound

fondamentale iniziare a trovare, costruire e testare una si basano su "messaggi push" per raggiungere direttamente

strada verso i vostri clienti dal primo giorno. Ci sono svariati i clienti.

canali distributivi: alcuni potrebbero essere inapplicabili Esempio di Canali Inbound:

nella fase iniziale della vostra startup, mentre altri possono Blogs, SEO, E-

books, white paper, webinar.

essere fattibili durante le fasi successive del suo avvio.

Esempio di Canali Outbound:

GRATIS contro A PAGAMENTO

SEM, annunci stampa Radio TV , fiere, telemarketing.

Prima di tutto chiariamo un concetto: non esistono sistemi

gratis. I canali “gratis” come il SEO, i social media e i blog,

hanno comunque un costo di risorse

umane per mantenerli.

Considerando un canale a pagamento come SEM, tipo

Google Adwords. Una volta si riusciva a ottenere dei risultati

significativi con 10 Euro al giorno: purtroppo oggi la festa

è finita e per la maggior parte dei prodotti la concorrenza

delle parole chiave è così feroce, che bisogna veramente

impegnarsi per prevalere.

166

KP

KS

VP

KR

CS

la

Soluzioni

Relazione

Problemi

la Proposta

i Segmenti

KM

di Valore

CH

di Clienti

la Metrica

i Canali

C$

R$

i Costi

i Ricavi

La Relazione

La Relazione con i clienti per una startup.

Nella prima fase della startup è necessario trovare i potenziali

clienti (prospects) con cui parlare. Occorre ricordare di

essere alla ricerca di persone afflitte da un problema e che,

di conseguenza, dovrebbero essere

disposte a pagare per

avere la vostra soluzione. Come si fa a trovare e raggiungere

i clienti potenziali? Non c'è una risposta giusta, una formula

magica. Dipende dalle risorse disponibili, da quanti contatti

registrati nei social avete, da quanti soldi, quanto tempo, e da

quale pensate sia il modo migliore per raggiungere i clienti.

L'obiettivo, a questo punto non è quello di testare i metodi di

acquisizione dei clienti, ma più semplicemente di acquisirli!

167

KP

KS

VP

KR

CS

la

Soluzioni

Relazione

Problemi

la Proposta

i Segmenti

KM

di Valore

CH

di Clienti

la Metrica

i Canali

C$

R$

i Costi

i Ricavi

I Ricavi e i Costi

Un sacco di fondatori posticipano la "questione dei prezzi" **Inizia con un prezzo unico**

perché non pensano che il loro prodotto sia pronto. Più volte Partire con i piani tariffari multipli è solo uno spreco di risorse:

si sente la frase: “come facciamo a farci pagare per un MVP?”

creare dei piani differenziati significa, nella maggior parte

I’MVP dovrebbe risolvere grossi problemi del segmento delle volte, dover scrivere codice per gestire la funzionalità di

di clienti identificato e quindi, per definizione, l’MVP deve segmentazione. Quando si è agli inizi, non si dispone ancora

offrire un valore sufficiente a giustificare la spesa.

di informazioni sufficienti per sapere come segmentare

Se c'è l'intenzione di essere pagati per il prodotto, è meglio correttamente il set di funzionalità in piani multipli.

farlo da subito per quattro motivi: soddisfare le giuste

aspettative, fissare un impegno verso il cliente, iniziare a **Utilizzare il piano "Prova Gratuita"**

generare flussi di cassa, ma il più importante di tutti è quello Offrire una via di entrata a una soglia nulla ma a tempo, in

di iniziare subito ad affrontare una delle parti più rischiose modo da poter forzare una decisione di conversione che

del tuo modello di business.

permette di capire il reale utilizzo del prodotto.

Il prezzo del prodotto è allo stesso tempo una delle cose più

complicate e più importanti da inquadrare.

Scegli un prezzo per testare

Il prezzo è parte integrante del prodotto, è più arte che scienza Le alternative

esistenti creano dei “punti di riferimento”

(si veda il libro di @NeilDavidson Don’t Just Roll the Dice).

nella mente dei clienti che essi useranno per classificare la

Il prezzo non è diverso da tutti gli altri elementi del BMC e soluzione proposta, quindi è importante capire e posizionare

perciò occorre dedicargli la stessa attenzione, applicando lo il prezzo in modo fortemente concorrenziale.

stesso metodo del Costruisci - Misura - Impara che abbiamo

utilizzato per ogni elemento del modello di business.

168

Considera i costi

L’obiettivo finale è trovare un modello di business scalabile

che si paghi, quindi forse è il caso di considerare il costo del

servizio.

Nel settore software la regola d’oro è che il lifetime value dei

clienti deve superare il costo di

acquisizione di almeno tre

volte.

E il Freemium?

Si tratta di un modello in cui si regala un'app e poi si fanno

pagare per gli upgrades. Sulla carta può apparire perfetto ma

la realtà è ben diversa.

Agile (scale)

I principi generali del metodo Agile

Il Manifesto Agile:

Il Metodo Agile è un particolare approccio alla gestione • La nostra massima priorità è soddisfare il cliente

dei progetti che viene utilizzato nello sviluppo del

rilasciando software di valore, fin da subito e in maniera

software. Questo metodo aiuta i team a rispondere

continua.

all'imprevedibilità della costruzione di software tramite

l’utilizzo di sequenze di lavoro incrementali e iterative, • Accogliamo i cambiamenti nei requisiti, anche a stadi

comunemente note come sprint.

avanzati del o sviluppo.

• I processi agili sfruttano il cambiamento a favore del

Panoramica Agile dei processi e dei metodi

vantaggio competitivo del cliente.

Qui di seguito si trova una panoramica del processo Agile

(e quello che è stato chiamato “Agile Project Management • Consegnamo frequentemente software funzionante, con

per principianti”) così come una semplice definizione della

cadenza variabile da un paio di settimane a un paio di

metodologia Agile per tutti i principianti che iniziano a

mesi, preferendo i periodi brevi.

progettare e sviluppare software, o per coloro che vogliono • Committenti e sviluppatori devono lavorare insieme

integrare la metodologia nella loro agenzia di SEO enterprise

quotidianamente per tutta la durata del progetto.

o web design company.

• Fondiamo i progetti su individui motivati.

Il metodo Agile definito

Lo sprint è un periodo di tempo assegnato ad una particolare • Diamo loro l'ambiente e il supporto di cui hanno bisogno

fase di un progetto. Gli sprint sono

considerati completi

e confidiamo nel a loro capacità di portare il lavoro a

quando il periodo di tempo scade. I membri del team possono

termine.

essere in disaccordo sul fatto che lo sviluppo sia soddisfacente • Una conversazione faccia a faccia è il modo più efficiente

o meno, tuttavia non ci sarà più lavoro su quella particolare

e più efficace per comunicare con il

team ed al ’interno

fase del progetto. Le fasi restanti del progetto continueranno

del team.

a svilupparsi nei rispettivi periodi di tempo.

• Il software funzionante è il principale metro di misura di

• La semplicità - l’arte di massimizzare la quantità di

progresso.

lavoro non svolto - è essenziale.

• I processi agili promuovono uno sviluppo sostenibile.

• Le architetture, i requisiti e la progettazione migliori

emergono da team che si auto-organizzano.

• Gli sponsor, gli sviluppatori e gli utenti dovrebbero

essere in grado di mantenere indefinitamente un ritmo

• A interval i regolari il team riflette su come diventare

costante.

più efficace, dopodiché regola e adatta il proprio

comportamento di conseguenza.

• La continua attenzione al ’eccel enza tecnica e al a

buona progettazione esaltano l’agilità.

Storia del Metodo Agile

Molte delle idee Agile sono emerse negli anni ‘70.

Sono stati condotti studi e revisioni sul Metodo Agile che spiega

la sua nascita come reazione nei confronti degli approcci

tradizionali allo sviluppo di progetti.

Nel 1970 il Dr. William Royce pubblicò un documento che

discuteva la gestione e lo sviluppo di grandi sistemi software.

L'articolo delineava le sue idee specifiche sullo sviluppo

sequenziale. In particolare, la sua presentazione affermava

che un progetto poteva essere sviluppato come un prodotto

su una catena di montaggio: ogni fase dello sviluppo doveva

essere completata prima di poter iniziare la fase successiva.

L'idea richiedeva che gli sviluppatori dovessero prima

mettere insieme tutti i requisiti di un progetto. Il passo

successivo consisteva nel completare la sua architettura.

Seguiva la scrittura del codice e le

sequenze di sviluppo

continuavano con incrementi finalizzati a chiudere parti

integrali di progetto. Quando queste fasi sono completate,

c’è poco o nessun contatto tra i gruppi specializzati che

completano ogni fase del progetto.

I pionieri del Metodo Agile credevano che se gli sviluppatori

avessero studiato il processo, avrebbero trovato la soluzione

più logica e utile per lo sviluppo del software.

172

Aziende che usano il Metodo Agile

Anche se non esiste un elenco ufficiale delle aziende che

utilizzano il Metodo Agile per i loro progetti, IBM è una delle

aziende che si serve apertamente di questo metodo per

sviluppare software. Di fatto molte aziende lo adottano

all’interno della loro struttura di sviluppo, ma non sono

sempre aperte sulla loro scelta di utilizzarlo.

Secondo IBM, l’uso del Metodo Agile genera significativi

cambiamenti organizzativi. IBM è convinta del fatto che

molti team di sviluppo software Agile aumenteranno le loro

possibilità di successo collaborando con una guida affidabile.

Tale azienda, inoltre, aiuta i clienti ad

implementare le

proprie strategie di sviluppo software Agile per i loro progetti

e fornisce una guida critica che aiuterà i team di sviluppo

software di Agile ad evitare le trappole comuni di adozione,

espansione e implementazione.

Vantaggi dell'uso del Metodo Agile

richieste di un cliente. Si adatta facilmente alle mutevoli

esigenze in tutto il processo, misurando e valutando lo stato

Il Metodo Agile nasce dall'esperienza con i progetti reali dei di un progetto. La misurazione e la valutazione permettono

principali professionisti del software del passato. Per questo infatti una visibilità accurata e tempestiva sull'avanzamento

motivo, le sfide e i limiti dello sviluppo tradizionale sono stati di ogni progetto.

scartati. Successivamente, il Metodo Agile è stato accettato Si potrebbe affermare che il Metodo Agile aiuta le

dall'industria come soluzione migliore per lo sviluppo di aziende a costruire il prodotto giusto: invece di cercare di

progetti e quasi tutti gli sviluppatori di software hanno usato commercializzare il software prima che venga scritto, il

il Metodo Agile in qualche forma.

Metodo Agile consente ai team di ottimizzarne il rilascio

Questo metodo offre una struttura leggera per assistere i durante il suo sviluppo e questo permette al prodotto di

team, aiutandoli a funzionare e a

mantenere l’attenzione sulla essere il più competitivo possibile sul mercato. Per tali motivi

rapidità di consegna. Questo focus aiuta le organizzazioni il Metodo Agile risulta un’opzione di sviluppo interessante sia

a ridurre i rischi complessivi associati allo sviluppo del per gli stakeholder che per gli sviluppatori.

software.

Ci sono molti critici del Metodo Agile, tuttavia esso produce

Il Metodo Agile assicura che il valore sia ottimizzato durante risultati che i

clienti possono portare in banca. Anche se

tutto il processo di sviluppo. L'uso della pianificazione un progetto può non essere esattamente come il cliente

iterativa e del feedback si traduce in team in grado di lo immagina, in ogni caso sarà consegnato entro il tempo

allineare continuamente un prodotto consegnato alle necessario per la sua realizzazione. Durante l'intero processo,

il cliente e il team adatteranno i requisiti ai fini di produrre la

qualità richiesta dai clienti stessi. Il

cambiamento continuo

a volte può dare sia al cliente che al team più di quanto

originariamente previsto per il prodotto. Per questi motivi,

il Metodo Agile è davvero una soluzione vincente per tutti

coloro che sono coinvolti nello sviluppo del software.

Agile

08

Capitolo Ottavo

Conclusioni

Blockchain: un nuovo inizio per le Aziende

FARE **Business** CON LA **Blockchain**

Capitolo Ottavo

Conclusioni

Blockchain: un nuovo inizio

per le Aziende

Siamo arrivati alla conclusione e a Febbraio 2019, in Italia Questo è anche un'enorme, enorme, enorme passo avanti per

è successo un fatto interessante: è stata approvato il le amministrazioni centrali e locali e per tutte le organizzazioni

"DL Semplificazioni" che dà valore legale alla tecnologia imprenditoriali italiane, per quanto riguarda lo scambio di

Blockchain e agli Smart Contracts.

documenti e firme elettroniche.

Nel Gennaio 2019 l'Italia è stata tra i primi paesi al mondo a

Questo è un enorme passo avanti per me, in quanto ho rendere obbligatoria la fatturazione elettronica per tutte le

passato gli ultimi quattro anni della mia vita a progettare imprese. Sì, ammetto che questo modo di fare innovazione

e sviluppare una soluzione basata sulla Blockchain per lo utilizzando il codice penale può sembrare estremo, ma se

scambio di documenti aziendali

chiamata Commercio. l'unico modo per innovare in Italia è quello di rendere un

network.

comportamento criminale non adeguarsi al futuro, beh, forse

Questo è anche un'enorme, enorme passo avanti per tutti il fine giustifica i mezzi, seguendo la filosofia di Machiavelli.

gli italiani, dal momento che tutti noi viviamo nel secondo

peggior paese burocratico del mondo (il Venezuela ci ha

battuto) almeno secondo il World Economic Forum.

Questo ci dà un raggio di speranza, perché il cambiamento

può aumentare l'efficienza se è nella giusta direzione.

178

Che cosa potrebbe cambiare concretamente per gli italiani a considerare i contratti intelligenti come giuridicamente

questa legge Blockchain? In poche parole, alla fine saremo vincolanti.

in grado di fare più cose online, tutto ciò che ho descritto in Questo ha un impatto enorme per due motivi:

questo libro, da oggi ha una copertura legale.

• Riconosce che gli Smart Contracts hanno lo stesso valore

contrattuale dei documenti digitali.

Le aziende possono usare la Blockchain per la firma e

esecuzione di:

• Si estende la sua applicabilità, in quanto possono essere

utilizzati in tutti i casi in cui la legge richieda la forma

• Contratti commerciali

scritta.

• Contratti di lavoro

Questa legge Blockchain potrebbe spingere lo sforzo per

• Contratti finanziari

trasformare digitalmente l'Italia realizzando le 100 cose da

• Contratti assicurativi

fare sulla Blockchain (Capitolo 3, pagina 70) che ora sono

- **Contratti bancari**

ancora presenti nei registri cartacei. In conclusione come

sostenitore dal 2008 del paradigma della Blockchain oggi,

La maggior parte dei registri pubblici può essere spostata a differenza degli altri giorni, sorrido pensando al futuro.

su una Blockchain e rendere la notarizzazione digitale una

commodity.

Il vantaggio più semplice e immediato è la marca temporale

digitale per tutti. Da oggi potremo certificare la data e l'ora

dell'esistenza di un documento digitale come prova basata

sulla Blockchain in un dato momento. In Italia dal 1862

esiste l'Ufficio del Registro, un ufficio con lo scopo di essere il

registro di tutte le cose, possiamo pensare che sia una proto-

Blockchain storica. Ogni giorno c'è ancora gente in Italia che

si mette in fila agli uffici postali per acquistare francobolli per

avere un documento timbrato e certificare la data.

La nuova legge sarà anche la prima nell'Unione Europea

Un grande ringraziamento finale al team di talenti

che hanno contribuito a realizzare questo libro:

SILVIA SERACINI

ANTONIO FACCI

NADIA BRAVO

PIERLUIGI SCOTOLATI

ANGELA VALMORBIDA

EGIDIO CASATI

RICCARDO MONTAGNIN

RAFFAELLA TALIN