LUISS

Dipartimento di Impresa e Management

Cattedra Economia e Gestione delle Imprese

La tecnologia blockchain al servizio dell'industria degli eventi dal vivo: Web3.0, Dapps in risposta al Secondary ticketing ed ad altre problematiche del settore

RELATORE

Prof. LUCA PIROLO

CANDIDATO

MATTEO RUBINO

MATR. 202291

ANNO ACCADEMICO 2021 / 2022

LA TECNOLOGIA BLOCKCHAIN AL SERVIZIO DELL'INDUSTRIA DEGLI EVENTI DAL VIVO: WEB3.0, DAPPS IN RISPOSTA AL SECONDARY TICKETING ED AD ALTRE PROBLEMATICHE DEL SETTORE

INDICE

INDICE

INTRODUZIONE

1. IL MERCATO SECONDARIO E LE SUE CARATTERISTICHE

1.1 Il mercato primario
1.2 La variabile prezzo
1.3 Il processo organizzativo
1.4 Il mercato secondario
1.5 Gli attori del mercato secondario
1.6 Le interazioni tra agenti del mercato primario e agenti del mercato secondario
1.7 Gli utilizzatori del mercato secondario
1.8 Gli speculatori
1.8.1 Come si riforniscono i grandi speculatori
1.8.2 Funzionamento e vantaggi del mercato secondario
1.9 I lati negativi del mercato secondario
1.9.1 Un mercato torbido
1.10 Soluzioni per arginare la rivendita speculativa

2. LA GENESI DELLA BLOCKCHAIN

2.1 Il contesto storico
2.2 Come funziona una blockchain
2.3 Architettura di una blockchain
2.3.1 Elementi generici di una blockchain
2.4 Funzionamento di una blockchain
2.4.1 La creazione di un blocco
2.5 Il consenso
2.5.1 I meccanismi di consenso
2.5.2 Tipologie di meccanismi di consenso nella blockchain
2.6 Smart contracts
2.7 Oracoli
2.7.1 Il funzionamento di un oracolo
2.7.2 Prova di autenticità
2.7.3 Tipologie di oracoli
2.7.4 Il problema della fiducia negli oracoli

3. L'APPLICAZIONE DELLA BLOCKCHAIN AL MERCATO DEGLI EVENTI DAL VIVO

3.1 Proposte e riflessioni

3.2 Revisione della letteratura

3.2.1 TickEth

3.2.2 Un'implementazione alternativa

CONCLUSIONE

BIBLIOGRAFIA

INTRODUZIONE

Gli eventi dal vivo costituiscono il motore economico portante dell'industria musicale del terzo millennio. Questa situazione è una conseguenza dell'avvento delle piattaforme di streaming con cui, allo stesso costo di un vecchio CD al mese, è possibile accedere a tutta o quasi la musica incisa durante la storia umana. Per chi fruisce il contenuto è sicuramente un'ottima soluzione, infatti in un certo senso la musica è democratizzata e resa accessibile a tutti anche gratuitamente se disposti a farsi interrompere dalle pubblicità. Dalla parte opposta abbiamo un'aristocratizzazione del settore degli eventi dal vivo per due principali motivazioni. In primo luogo l'industria discografica riceve un compenso irrisorio dagli ascolti effettuati sulle piattaforme di streaming e si è vista costretta ad aumentare il costo dei biglietti per poter restare in attivo. In secondo luogo è accaduto che l'ingegno e l'inclinazione al profitto umane hanno portato ad una evoluzione del cosiddetto bagarino che sin da quando sono esistiti gli eventi a pagamento, ha distribuito dietro laute ricompense ed a volte al miglior offerente gli ultimi biglietti rimasti durante le ore precedenti all'evento, posizionandosi nelle immediate vicinanze del luogo in cui si sarebbe svolto. Il bagarino 2.0 sfrutta in pieno la rivoluzione informatica e di internet, si avvale, infatti, di automazioni che gli consentono di acquistare in grossi lotti i biglietti non appena sono resi disponibili. In questo modo i siti di vendita primaria vengono letteralmente prosciugati ed il traffico viene riversato sulle piattaforme del mercato secondario. Questi spazi virtuali sono il regno ed il terreno di caccia ideale dei nuovi bagarini che operano a volte anche con la connivenza sia della stessa piattaforma che degli agenti primari. I prezzi dei biglietti su questi siti-rivenditori sono naturalmente maggiorati soprattutto per gli eventi più esclusivi, dove le percentuali di guadagno per lo speculatore diventano vertiginose. Per anni le istituzioni e le aziende appartenenti al mondo della musica hanno provato a limitare questo fenomeno con varie soluzioni più o meno valide. La stessa tecnologia che ha messo in difficoltà questo settore ha partorito quella che sembra candidata ad essere una delle maggiori rivoluzioni di questo secolo. Nel 2008 Satoshi Nakamoto, molto probabilmente uno pseudonimo che racchiude un gruppo di individui, ha pubblicato un paper con cui condivideva al mondo l'invenzione del Bitcoin. Ci sono voluti alcuni anni affinché la tecnologia che ne permette il suo funzionamento, la blockchain, fosse compresa a pieno nelle sue possibilità. Le generazioni "Millennial" e "Z" per diversi motivi vedono nel sistema blockchain una struttura affidabile e capace di ridurre gli errori a zero. Essa infatti alleggerisce le nostre menti dal peso della fiducia grazie alla sue implicite caratteristiche: è immutabile, decentralizzata, sicura e trasparente. Nel seguente elaborato proveremo ad applicare le sue peculiarità intrinseche al

mercato degli eventi dal vivo con la volontà di risolverne i suoi attuali problemi.

1. IL MERCATO SECONDARIO E LE SUE CARATTERISTICHE

L'obiettivo che il primo capitolo si prefigge di raggiungere è quello di realizzare una panoramica sul problema che si discuterà in questo elaborato. Il settore della musica dal vivo rappresenta un momento culturale fondamentale dell'epoca moderna ed un'esperienza d'arte fruita da centinaia di persone in tutto il mondo. Non solo: è anche un'industria che globalmente dà lavoro a milioni di persone. Basti pensare all'eccitazione dei fan in tutto il mondo che aspettano ore in piedi prima di poter vedere il proprio artista preferito esibirsi.

La storia della musica, infatti, vede il suo punto di partenza proprio nelle esibizioni dal vivo, che nel passato rappresentavano l'unico modo in cui si potesse fruire di questa forma d'arte. Con l'invenzione prima del fonografo e poi del grammofono e grazie alle evoluzioni nel mondo della tecnologia nell'800, il settore musicale e le relative possibilità di guadagno iniziarono a crescere esponenzialmente. In quel momento si verificò un cambiamento epocale che non avrebbe soltanto sconvolto il mondo della musica e dell'arte in generale, ma anche e soprattutto di come venivano percepiti e utilizzati i media dalla società. Le prime emittenti radiofoniche, istituite negli anni '20 e l'introduzione del mitico vinile negli anni '40, rappresentano soltanto l'inizio di una rivoluzione senza precedenti che arrivò a comprendere i moderni Compact Disk, fino alle recentissime piattaforme di streaming che hanno messo in crisi l'industria discografica moderna. È dunque al seguito di questa rivoluzione tecnica che anche il settore della musica dal vivo subisce dei fortissimi sconvolgimenti: da forma d'arte fruibile soltanto in un contesto sociale e dal vivo, la musica diventa a portata di tutti, fruibile nelle case di ognuno. Ed è proprio nel momento in cui le case discografiche stanno subendo le perdite più gravi inflitte dalle piattaforme online di streaming digitale, che il settore della musica dal vivo è stato visto come forte leva per risollevare i destini dell'industria musicale.

Anche però il settore della musica dal vivo mostra delle problematiche intrinseche: quella che in questa sede ci si propone di analizzare riguarda il secondary ticketing. Se è vero che da quando sono stati proposti i primi concerti a pagamento, si sono verificati atti di bagarinaggio, è anche vero che nell'epoca moderna questo fenomeno ha preso sempre più piede e più rilevanza avvalendosi degli strumenti potentissimi che derivano delle piattaforme digitali.

In questa tesi ci si propone di analizzare il fenomeno e di proporre come soluzione alle nuove forme di bagarinaggio il modello strutturale della blockchain.

1.1 Il mercato primario

Il punto di partenza della seguente analisi sarà il mercato primario dei biglietti per gli eventi dal vivo poiché dalle sue mancanze e specifiche caratteristiche scaturiscono le problematiche del secondario. I prezzi, il modo in cui vengono distribuiti i biglietti e la capacità delle venue di far rispettare le condizioni di entrata sono i fattori principali che influenzano la portata e le caratteristiche del mercato secondario.

1.2 La variabile prezzo

La determinazione del prezzo è un processo delicatissimo specialmente nel mercato della cultura e delle esperienze dal vivo. Come suggerisce Alan Krueger nel suo "Rockonomics", l'armonia del mercato applicato alle emozioni diventa incredibilmente difficile da raggiungere e precaria. A questo proposito nel 2006 Terry Barnes, l'allora presidente di ticketmaster, dichiarò che quello in cui operava la sua azienda era il settore peggiore nel determinare e applicare i prezzi. Una delle motivazioni principali che Barnes apportò fu quella secondo la quale i musicisti non considerino eticamente giusto proporre i prezzi che derivano dall'incrocio tra domanda ed offerta, ritenendoli troppo alti per convinzioni ideologiche, secondo le quali l'arte dovrebbe essere fruibile facilmente a tutti. Considerate però le cifre altissime a cui in tantissimi casi sono stati rivenduti migliaia di biglietti per eventi dal vivo nel mercato secondario, si può facilmente dedurre come la domanda dia contro alle ideologie dei musicisti. Alan Krueger trova una sintesi a queste dinamiche definendo gli eventi musicali come "economie da festa di quartiere" in cui gli invitati contribuiscono alle spese ma nelle quali sarebbe socialmente ed eticamente intollerabile se da queste azioni spontanee gli organizzatori ne traessero profitto. Marc Geiger, dirigente ed imprenditore musicale, cofondatore del famosissimo e seguitissimo festival musicale "Lollapalooza", invece, definisce la tendenza degli artisti a ritenere troppo alti i prezzi a cui i biglietti vengono rivenduti sul mercato secondario e che quindi incrociano l'attuale domanda, un eco da "socialismo del rock'n'roll".

Possiamo infatti considerare un titolo di partecipazione ad un evento come un bene di lusso emozionale: nessuno costringe gli acquirenti ad accettare un qualsiasi prezzo, ma loro sono spinti da un impulso emotivo che li trascina a comprare anche al di sopra delle proprie possibilità e nel caso in cui vengano acquistati i biglietti nelle prime file entra il gioco anche l'intento di dimostrare uno status sociale elevato.

I promoter e gli organizzatori degli eventi dal vivo fissano i prezzi per conto dell'artista o in generale per conto dell'evento stesso. A seconda del luogo designato e della strategia di marketing possono esserci varie fasce di prezzo: tendenzialmente nei teatri infatti si ha il maggiore scarto tra i posti più vicini e quelli più lontani dal palco. Lo scarto di cui sopra comprende spesso il valore nominale del biglietto e le spese aggiuntive che vanno a coprire le spese necessarie all'organizzazione dell'evento stesso, che generalmente sono poi distribuite tra gli organizzatori. Questi ultimi vorranno sicuramente massimizzare il guadagno dai posti che hanno a disposizione ma d'altra parte è nei loro interessi anche vendere tutto il prima possibile per sfruttare al massimo l'ondata pubblicitaria e del passaparola. In particolar modo i promoter adotteranno la strategia del "tutto subito", poiché generalmente vanno a margine solo una volta venduti la maggioranza dei biglietti. Inoltre prezzi bassi possono anche essere imposti per stimolare la domanda ed aggiungere date nello stesso luogo o nelle vicinanze.
È anche vero però che varie analisi riportano che maggiore è il costo di entrata, minori saranno i ricavi dalle vendite di merce promozionale e minori saranno le possibilità di una partecipazione futura ad un evento dello stesso artista. Questo risultato però spesso si scontra con gli obiettivi degli artisti che, anche in chiave lucrativa, vogliono spostarsi in arene sempre più grandi, avendo quindi bisognoso di attrarre sempre più pubblico e di consolidare il vecchio. Un'opinione diffusa nel mondo della musica è che siano proprio i sostenitori con un reddito più basso a creare la giusta atmosfera per mettere l'artista nelle condizioni di esibirsi al meglio. Fissare prezzi bassi quindi oltre ad essere socialmente giusto ed utile può avere diversi vantaggi per artisti organizzatori e promotori, portando però ad un'istituzione sempre maggiore del mercato secondario. Attualmente manca infatti, nella maggior parte dei casi, un'adeguata implementazione di sistemi atti a disinnescare le speculazioni.

1.3 Il processo organizzativo

Nell'organizzazione dei concerti di grandi artisti solitamente questi ultimi sono affiancati da almeno un manager che li rappresenti, un'agente che si occupa del booking delle varie venue, pronto a negoziare con un promoter che si occupa di organizzare il tour nelle date e nei luoghi contrattando a sua volta con i teatri e i gestori dei locali. In base alla domanda prevista si decideranno le modalità e le tempistiche di distribuzione dei biglietti. Artista, manager e agente di prenotazione si accorderanno su fasce di prezzo dei vari posti, mentre per la distribuzione dei biglietti solitamente venue e promoter dividono con

percentuale 60/40 l'onere e onore. Il promotore cede la sua quota ad una o più biglietterie in cambio di una percentuale sui guadagni e la sede dell'evento la smercia attraverso il suo sito web.

Il promotore è colui che si addossa il rischio di impresa poiché affitta il palcoscenico e ingaggia l'artista, inoltre è soggetto al mutamento dei gusti quindi ad una difficile valutazione della domanda. Secondo i dati di organi rappresentativi di settore, un promotore va in profitto solo sull'ultimo 10-15% delle vendite, quindi, è anche nel suo interesse tenere i prezzi bassi in modo da riempire completamente le arene.

I locali solitamente sostengono costi fissi e percepiscono un affitto predeterminato durante la fase di contrattazione col promotore, giocando su variabili come il giorno della settimana e la portata della lista iscritti alle comunicazioni del locale.

Nell'era della post-pirateria e del "non possesso", per gli artisti le esibizioni rimangono la maggiore se non l'unica fonte di guadagno, quindi, è molto importante soprattutto per loro massimizzare il ritorno su questi eventi.

1.4 Il mercato secondario

Chiariti tutti i player che hanno sono stakeholders nell'industria della musica dal vivo, a questo punto entra in gioco il mercato secondario dove utenti o organizzazioni con finalità diverse metteranno in vendita i biglietti acquistati sul mercato primario. Internet ha reso possibile la creazione di piattaforme appositamente dedicate che rendono lo scambio semplice e fluido ed inoltre il consumatore è oggigiorno assai avvezzo agli acquisti effettuati tramite questo mezzo.

1.5 Gli attori del mercato secondario

Nel mercato secondario del ticketing operano varie tipologie di agenti:

- Piattaforme create dal distributore primario in cui gli interessati possono scambiarsi i titoli.

  Siti come "Twickets" e "Scarlet mist" che applicano basse o assenti commissioni finanziandosi con la pubblicità e in cui gli scambi avvengono al valore nominale più le spese sostenute sul primario, tra sostenitori onesti desiderosi di ripagarsi il costo di un biglietto che non potranno più utilizzare, dando la possibilità ad un loro pari di

partecipare all'evento. Basandosi sul rispetto e sulla fiducia queste piattaforme non offrono alcun tipo di garanzia. Dall'indagine del professor Waterson risulta che questi siti attraggono una quota minoritaria del traffico.

- Le piattaforme commerciali di rivendita che richiedono ingenti commissioni e sono incentivate ad attrarre grandi volumi di biglietti. Alcune tra le più conosciute sono: "StabHub" di "eBay", "GETMEIN!" di "Ticketmaster" e "Viagogo". Sono ormai delle realtà affermate nel settore della biglietteria e del commercio in rete e sostengono di non avere alcun legame con gli speculatori, ma invece di fornire un servizio di garanzia e ritardo di acquisto. Queste piattaforme di secondary ticketing applicano commissioni molto maggiori del primario, fino al 25-30% in totale tra acquirenti e venditori giustificate dalle garanzie che offrono come sostituzione e rimborso, compreso il caso di frode, quando dovrebbero anche denunciare il fatto alle autorità competenti. Secondo le dichiarazioni di "StubHub" solo il 4% di chi ha acquistato sul loro sito è dovuto ricorrere alla garanzia. Generalmente le società di scambio trattengono i guadagni del rivenditore finché l'acquirente non abbia partecipato con successo all'evento e se si presenti la necessità di sostituirlo addebitano i costi relativi al rivenditore. I grandi rivenditori sono, però, esuli da queste condizioni, poiché vitali per il funzionamento dei siti intermediari in quanto fornitori della quasi totalità dei biglietti disponibili, che generano traffico facendo guadagnare così da commissioni e pubblicità.

  A sostegno dei consumatori vi sono anche dei siti indipendenti, che comparano i prezzi del mercato secondario e forniscono recensioni sull'affidabilità dei rivenditori.

1.6 Le interazioni tra agenti del mercato primario e agenti del mercato secondario

Tra i due mercati, però, non mancano i momenti di incontro e questi non rappresentano sempre dei contatti sbagliati. Negli ultimi anni tramite il programma "Dispatches" e "Le Iene" è emerso che promoter, artisti e agenti, a volte all'oscuro dagli artisti, riforniscano sottobanco i siti di secondary ticketing. Nonostante ciò sia inaccettabile per il grande pubblico, questo metodo permette di non disperdere interamente il frutto del lavoro degli operatori primari a beneficio degli speculatori e consente ai promoter di piazzare

biglietti di eventi di poco successo a prezzi ridotti pur di riempire il locale e limitare le perdite.
La maggior fonte di guadagno per un locale deriva da parcheggio e zona ristoro, per questo alcune volte i gestori si ritrovano anch'essi sul secondario a svendere biglietti di eventi a bassa richiesta per aumentare l'afflusso di gente e quindi le suddette entrate.

1.7 Gli utilizzatori del mercato secondario

Per quanto riguardo prettamente il mercato secondario, al suo interno vi troviamo tre macro-tipologie di utenti:
-gli appassionati che non hanno più la possibilità di assistere all'evento del proprio artista preferito e sono disposti ad acquistare anche a prezzo maggiorato un biglietto per un determinato evento;
-gli appassionati che vogliono andare all'evento ma che comprano anche più biglietti di quelli di cui necessitano per limitare o azzerare la spesa rivendendo a margine quelli in eccesso;
-i rivenditori professionisti totalmente disinteressati all'evento o all'artista, ma che sono sul mercato soltanto per trarne profitto. Questa è la categoria della quale ci interesseremo maggiormente nelle prossime pagine.

1.8 Gli speculatori

Le ultime due categorie degli utilizzatori del mercato secondario, interessate meramente al profitto seppur con motivazioni diverse, renderanno subito disponibili i biglietti in loro possesso in modo da aver il maggior tempo possibile per la rivendita e per sfruttare la promozione implementata dagli operatori del primario. Questi possono essere sia speculatori "da cameretta" sia delle vere e proprie organizzazioni, che approfittano della complicità delle piattaforme di rivendita per riuscire a non essere identificati.

1.8.1 Come si riforniscono i grandi speculatori

Le grandi organizzazioni che operano sul mercato secondario si riforniscono dei biglietti in vari modi:

1. Sfruttando le loro conoscenze nell'industria musicale o addirittura facendone parte come lavoratori;
2. Avendo una squadra di lavoratori creata appositamente per comprare il massimale consentito ad una persona singola, magari utilizzando anche l'accesso alle prevendite;
3. Servendosi di automazioni digitali create apposta per acquistare potenzialmente tutto l'inventario disponibile, aggirando ogni tipo di limitazione.

1.8.2 Funzionamento e vantaggi del mercato secondario

Solitamente i veri sostenitori dell'artista acquistano i propri biglietti molti mesi prima dell'evento, durante la vendita generale. Coloro che per varie motivazioni non riuscissero più ad essere in grado di assistere all'evento sono i clienti ideali per cui originariamente, almeno in teoria, sono state implementate le piattaforme di rivendita; inoltre danno la possibilità a utenti interessati di poter programmare all'ultimo momento, in base ai propri impegni, la partecipazione all'evento e di avere una opzione di acquisto flessibile, molto più sicura dei tradizionali bagarini di strada. Fatta eccezione per gli eventi più popolari, i prezzi tendono ad essere maggiori subito dopo il rilascio iniziale per ridursi gradualmente anche al di sotto del valore nominale a qualche ora dall'evento. Per gli eventi popolari tali consumatori saranno disposti a pagare cifre di molto superiori al valore nominale mentre per quelli meno popolari potranno trovare sempre più occasioni via via che la data di esibizione si avvicini.
Tuttavia, il mercato secondario offre un'importante risorsa agli attori del primario ovvero una verificata prova del prezzo di mercato per ogni posto nel luogo dell'evento. Ogni consumatore dispone di una percezione diversa del valore di un evento live, quindi, è naturale che ci siano prezzi variabili nello spazio e nel tempo. Possiamo individuare due macrocategorie in questo senso: coloro che organizzano i propri impegni in base all'evento e coloro che partecipano all'evento in base ad essi. Generalmente i primi hanno meno disponibilità economica ed una percezione più bassa del valore del proprio tempo, quindi, parteciperanno alla vendita primaria mesi prima dell'evento. I secondi avendo maggiori disponibilità e maggior considerazione del proprio tempo, si affideranno al mercato secondario per partecipare all'evento solo dopo che avranno certezza di poterlo fare. Questi ultimi saranno naturalmente più inclini a pagare un sovrapprezzo per il servizio di elasticità temporale offerto.
Le piattaforme di scambio rendono un servizio utile alla comunità di fan e appassionati e l'intento di questa ricerca è trovare un modo di arginare chi provenendo sia dall'interno che

dall'esterno dell'industria musicale sfrutti e monetizzi in maniera parassita il lavoro e la popolarità dei professionisti del settore.

1.9 I lati negativi del mercato secondario

Il mercato secondario presenta sicuramente degli inconvenienti intrinsechi. Gli operatori coinvolti nell'evento non riceveranno alcuno dei profitti realizzati sul secondario e perderanno la possibilità di instaurare delle relazioni coi consumatori finali da cui potrebbero trarre vantaggiose informazioni e contemporaneamente offrire loro promozioni mirate.
La maggior parte dei clienti del mercato secondario lamenta l'eccessivo sovrapprezzo sui biglietti che limita l'accesso alle classi meno abbienti.
In vari modi può far ritrovare senza un biglietto i sostenitori. Gli operatori del secondario, infatti, offrono gli stessi biglietti su diverse piattaforme per aumentare i profitti e le possibilità di vendita, quindi, potrebbe accadere che non riescano a trovare un biglietto sostitutivo. Un serio problema nel mercato secondario è quello delle frodi, infatti, in molti siti compaiono rivenditori o singoli che vendono biglietti contraffatti o totalmente inesistenti. I grandi rivenditori coi loro metodi di acquisto massivo tolgono la possibilità al pubblico che lo volesse, di ottenere biglietti nelle vendite primarie.

1.9.1 Un mercato torbido

Molti dei problemi del mercato secondario derivano dalla poca informazione della clientela e dalla poca trasparenza degli attori primari e secondari. Emerge da varie indagini che il consumatore ha scarsa conoscenza delle dinamiche del mercato e dei suoi attori.
Nell'organizzazione dell'evento musicale le venue richiedono ai promoter di controllare la distribuzione dei biglietti, ciò comporta la creazione di una pluralità di fonti primarie da cui il consumatore trae confusione. Sarebbe utile se tramite fonti ufficiali si informasse il pubblico su quali siano gli agenti autorizzati alla distribuzione primaria e invitasse a diffidare di qualsiasi altra fonte. Una ricerca del "Bostock Marketing Group ltd" rivela che quasi un quarto dei partecipanti riteneva il sito del secondario dove aveva comprato il titolo un distributore primario autorizzato con proprietà dei biglietti.
Bisognerebbe specificare al pubblico quanti dei biglietti siano effettivamente disponibili alla vendita generale, poiché la maggior parte delle volte questi sono la minoranza del totale;

infatti, molti sono stati offerti in prevendita a vari requisiti come: possedere un determinata carta di pagamento, essere membri di un fan club, di un promoter, di una venue, avere effettuato degli acquisti o preordinato un album in uscita. Negli stati uniti per alcuni eventi si attesta che l'85/90% dei biglietti siano distribuiti nelle prevendite e tra questi la maggior parte siano nelle posizioni migliori. Ulteriori biglietti saranno affidati agli agenti coinvolti in prima persona nell'evento come artista, manager, etichetta e simili.

1.10 Soluzioni per arginare la rivendita speculativa

Maggiormente al di sotto del prezzo di equilibrio saranno i prezzi del primario più rivenditori del secondario saranno attratti dai guadagni potenziali; quindi, per contrastarli bisognerà agire implementando limitazioni e controlli. Gli organizzatori dell'evento hanno poco potere riguardo la diffusione dei biglietti una volta venduti sul mercato primario.

Il modo più immediato che possa venire in mente per limitare la rivendita è quello di inserire un espresso divieto nei termini e condizioni del biglietto, ma questo per essere rispettato richiede un grosso sforzo da parte degli agenti coinvolti. Inoltre, è anche rischioso per gli organizzatori consentire la restituzione di un biglietto acquistato, poiché potrebbe far aumentare i costi. Si potrebbe limitare l'acquisto di biglietti per persona, ma questo è facilmente aggirabile e difficilmente controllabile, soprattutto in presenza di più agenti primari. Il consumatore è penalizzato, poiché corre il rischio di perdere il denaro speso in caso di inutilizzo del biglietto, anche se generalmente è accettato dagli organizzatori il fatto di cederlo a conoscenti.

Misure adottate nel primario che potrebbero diminuire le problematiche del secondario sono una maggiore differenziazione di prezzo e il ricorso ad estrazioni per i posti a maggior domanda.

Una efficace strategia per massimizzare il profitto e limitare il fenomeno degli speculatori sarebbe quella di applicare una tariffazione dinamica come accade nella vendita dei biglietti aerei. Un algoritmo si occuperà di calcolare l'esatto valore di ogni posto in base a parametri come la vicinanza al palco, la prossimità dell'evento, i posti restanti e la domanda in corso.

Un'altra arma anti-bagarini sarebbe quella di distribuire nel tempo le vendite come fatto dagli organizzatori e agenti del "reputation tour" di Taylor Swift che sono riusciti a ridurre drasticamente il numero di biglietti spostati sul secondario dal 30% del tour precedente al 3%.

Gli attuali sviluppi tecnologici permettono di implementare sistemi di riconoscimento biometrico all'entrata in modo da associare ogni biglietto ad un individuo e di bloccare gli acquisti effettuati da automazioni, ma essendo attualmente dei metodi onerosi le biglietterie e i locali non sembrano essere inclini a volerne sopportare la spesa.

2. LA GENESI DELLA BLOCKCHAIN

2.1 Il contesto storico

La crisi economica del 2007 aveva distrutto completamente l'allora concezione delle istituzioni e mercati finanziari. I sistemi centralizzati dei mercati finanziari, gestiti da grandi intermediari come banche e società di investimento, fallivano ed iniziavano a crollare. La fiducia nei mercati scese drasticamente scatenando il panico che portò al loro collasso. In questo contesto un'entità sotto lo pseudonimo di Satoshi Nakamoto realizzò per la prima volta al mondo una moneta che non necessitava di autorità centrale ed era amministrata alla pari dagli utilizzatori, il Bitcoin. La fiducia tra le parti era assicurata da un sistema che più tardi sarà chiamato blockchain e che si assicurerà di verificare, validare, registrare e tenere onesto il trasferimento di denaro. Bitcoin vide la luce nel gennaio 2009 ma l'idea di una moneta digitale risale alla stessa nascita di internet e la sua blockchain si basa su oltre 40 anni di ricerca. La bibliografia dello "white paper" (in seguito saranno chiamati così quei documenti che annunciano la nascita di una criptovaluta e ne spiegano il funzionamento) di Bitcoin contiene studi scientifici dal 1957 al 2002 su crittografia, hashing, reti tra pari e protocolli di consenso. Col tempo ci si è resi conto che la blockchain poteva essere utilizzata anche per trasferire e validare digitalmente altri beni quindi si è iniziato a costruire blockchain che consentivano la programmazione di app e contratti.

2.2 Come funziona una blockchain

Varie possono essere le definizioni corrette di blockchain. La definizione di Layman, una delle più apprezzate, enuncia che la blockchain sia un sistema di registrazione dei dati in continua crescita, sicuro e condiviso in cui ogni utente possiede una copia del registro che può essere aggiornata solo se tutte le parti coinvolte nella transazione sono consenzienti. La definizione tecnica la descrive come un registro distribuito tra pari crittograficamente sicuro, aggiornabile solo tramite aggiunta, estremamente difficile da modificare, aggiornabile solo tramite accordo o consenso tra le parti. Vediamo in dettaglio le caratteristiche principali della blockchain:

- PEER TO PEER

Consiste in una rete in cui non esiste un'autorità di controllo ed in cui tutti gli utenti possono comunicare direttamente tra loro. Questo consentirà agli utenti di scambiare dati come transazioni di denaro, senza la necessità di rivolgersi ad un intermediario.

- HA UN REGISTRO DISTRIBUITO

Ogni partecipante alla rete detiene una copia esatta di tutte le transazioni effettuate ovvero l'intero registro continuamente aggiornato.

- È CRITTOGRAFICAMENTE SICURA

La crittografia assicura che il registro sia al sicuro da manomissioni ed usi impropri. Nello specifico impedisce di repudiare dati, tiene intatta la loro integrità e ne autentica l'origine.

- HA REGISTRO DI SOLA AGGIUNTA

All'interno della blockchain possiamo aggiungere dati solo in sequenza temporale. Questo implica che una volta aggiunti dei dati è quasi impossibile modificarli. I blocchi della blockchain creano in questo modo un registro delle transazioni immutabile e a prova di manomissione. Solo se il 51% della potenza colludesse contro la blockchain potrebbe modificare il registro.

- È AGGIORNABILE TRAMITE CONSENSO

La caratteristica cruciale di una blockchain è essere aggiornabile solo tramite consenso. Vi sono vari algoritmi di consenso come proof of work e proof of stake che analizzeremo in seguito. Questi consentono di raggiungere un accordo tra le parti e farle accettare il fatto che quanto deciso e scritto nella blockchain sia vero. In questo modo si elimina la necessità di una autorità centrale poiché il registro centrale è controllato da questi meccanismi. Ogni cambiamento nella blockchain dovrà essere validato attraverso severi criteri predefiniti nel protocollo della blockchain e potrà esservi scritto solo dopo che sia stato raggiunto il consenso tra tutti i nodi partecipanti alla rete.

2.3 Architettura di una blockchain

Possiamo immaginare la blockchain e tutto ciò che ne rende possibile il suo funzionamento come un insieme di strati, dal generale al particolare avremo:

- Il network, solitamente Internet, che fornisce una base per le comunicazioni blockchain; un “peer to peer” network consistente in un insieme di protocolli di diffusione delle informazioni come il “flooding” e il “gossip”;
- la crittografia attraverso vari protocolli garantisce la sicurezza della blockchain giocando un ruolo fondamentale nell'integrità dei processi, nella diffusione sicura delle informazioni e nei meccanismi di consenso. Questo livello è costituito da crittografia a chiave pubblica e altre componenti rilevanti come funzioni di Hash e firme digitali;
- attraverso l'uso di vari meccanismi di consenso si assicura l’accordo tra i diversi partecipanti. I vari protocolli di consenso utilizzati possono essere lo State Machine Replication, quelli basati su prova, quelli di tolleranza al problema dei generali bizantini;
- grazie ai livelli descritti sopra la blockchain può avere delle funzioni di esecuzione come trasferimento di valore, generazione di blocchi, attuazione di contratti intelligenti attraverso “macchine virtuali”;
- infine lo strato delle applicazioni composto da applicazioni decentralizzate, DAOs ovvere organizzazioni autonome decentralizzate, contratti intelligenti, e agenti autonomi. In questo livello è possibile utilizzare ogni tipo di programma che operi su blockchain, nello specifico questo è consentito all’utente attraverso le applicazioni decentralizzate.

2.3.1 Elementi generici di una blockchain

Introduciamo i concetti fondamentali per descrivere la blockchain ed il suo funzionamento:

- Indirizzo, una chiave privata derivata da una chiave pubblica che consente di identificare in una transazione blockchain mandante e ricevente;
- Transazione, unità elementare di una blockchain, rappresenta un trasferimento da un indirizzo ad un altro;
- Blocco, varia nei suoi dettagli in base al tipo di blockchain, ma generalmente è composto principalmente da:
    - Testa del blocco:

        - riferimento al blocco precedente (eccetto per il blocco della genesi, ovvero quello decodificato al principio della blockchain);
        - “nonce”, un numero generato casualmente ed utilizzato una sola volta, molto comune nelle operazioni crittografiche in generale;
        - la marcatura temporale “timestamp” del momento in cui è stato creato il blocco;
        - radice di Merkle, l’hash di tutti i nodi di un albero di Merkle. I “Merkle trees” sono ampiamente utilizzati per convalidare dati di grosse dimensioni in maniera sicura ed efficiente; infatti, nella blockchain è possibile verificare l'intero storico delle transazioni presenti accertando unicamente la Merkle root;
    - Corpo del blocco:
        - Lista delle transazioni, ovvero la registrazione di un determinato evento. La quantità di transazioni includibili in un blocco dipende dal tipo di blockchain.
- Peer-to-peer network, una rete tra pari, una topologia di network in cui tutti i partecipanti possono liberamente inviare e ricevere messaggi tra loro;
- Linguaggio di programmazione, consente di istruire la blockchain a svolgere determinati compiti. Quello di bitcoin è chiamato “Script” e consente solo un numero limitato di operazioni,per questo è definito Turing incompleto. Un linguaggio di programmazione in grado di performare ogni tipo di operazione è definito turing completo, la prima blockchain ad averne uno è stata Ethereum con Solidity;
- Virtual Machine, consente ad una blockchain di essere programmata mediante un linguaggio Turing Completo;
- State Machine;
- Smart Contracts, contratti intelligenti, sono dei programmi eseguibili sulle blockchain provviste di virtual machine. Una volta programmati svolgono in automatico la loro azione ogni qualvolta le condizioni di attivazione si verifichino;
- Nodo, un programma che in base al suo ruolo ed al tipo di blockchain può svolgere varie funzioni come proporre e validare una transazione, facilitare il consenso e rendere sicura la rete. Ognuno di essi è in grado di comunicare con tutti gli altri nodi della rete.

2.4 Funzionamento di una blockchain

2.4.1 La creazione di un blocco

Un nodo inizia la transazione creando la sua chiave privata e poi firmando digitalmente con essa. In una blockchain una transazione può rappresentare diverse azioni. Abitualmente è un insieme di dati rappresentativi o il trasferimento di valore tra utenti della rete via criptovalute o l'attivazione di uno smart contract che svolge un'azione preconfigurata. Questi dati solitamente descrivono la dinamica del trasferimento, le regole pertinenti, indirizzo di mittente e destinatario, altre informazioni per la convalida.

La transazione, utilizzando protocolli di diffusione di dati, è propagata agli altri nodi che secondo criteri predefiniti la valuteranno. Una volta raggiunti i nodi miner, dei nodi speciali che risolvendo dei calcoli crittografici certificano le transazioni, questi valuteranno la transazione e la includeranno in un blocco dando il via al processo di mining ovvero di "estrazione" delle criptovalute. Quest'ultimo processo è talvolta definito ricerca del blocco. I nodi miner competono tra loro per chiudere il blocco che hanno creato attraverso il processo del mining. Una volta che il miner ha soddisfatto i requisiti del meccanismo di consenso, il blocco è considerato trovato e finalizzato quindi tutte le transazioni contenute confermate e valide. Solitamente nelle blockchain di criptovalute il nodo che ha trovato il blocco viene ricompensato con della moneta per le risorse e lo sforzo impiegati nel processo. Il blocco appena minato sarà validato, le transazioni o gli smart contract contenuti eseguiti e propagati agli altri partecipanti alla rete, che valuteranno ed eseguiranno il blocco. Quest'ultimo si collegherà crittograficamente al blocco precedente creando un "puntatore hash" divenendo quindi parte del registro blockchain.

2.5 Il consenso

In una blockchain è definito consenso distribuito quel processo in cui si raggiunge un accordo tra i nodi partecipanti riguardo lo stato finale dei dati, nonostante la presenza di nodi malevoli. Possiamo definirlo la colonna portante della blockchain poiché consente di

decentralizzare il controllo attraverso il processo opzionale del mining. In base alla tipologia di blockchain si utilizza un algoritmo di consenso diverso.

2.5.1 I meccanismi di consenso

Un meccanismo di consenso rappresenta quell'insieme di procedure svolte da tutti o quasi i nodi partecipanti atte a raggiungere un accordo sui dati proposti. Un meccanismo di consenso ha i seguenti requisiti:

- Accordo, uno stesso dato è supportato da tutti i nodi onesti;
- Integrità, ad ogni nodo è consentito prendere posizione una sola volta nel corso di un singolo ciclo di consenso;
- Validità, il valore deciso dal consenso distribuito deve essere per forza essere stato proposto inizialmente da almeno un nodo onesto;
- Tollerante ai guasti, l'algoritmo di consenso deve essere in grado di svolgere correttamente la sua funzione anche in presenza di nodi guasti o malevoli;
- Risoluzione, ogni nodo onesto partecipante deve terminare il processo di consenso ed infine prendere una decisione.

2.5.2 Tipologie di meccanismi di consenso nella blockchain

Esistono due macro tipologie di meccanismi di consenso ed entrambe fanno fronte ad ogni categoria di guasto da quelli arbitrari a quelli di blocco.

- Meccanismi di consenso basati sulle prove, richiedono ai nodi di competere in una lotteria che eleggerà casualmente basandosi su un algoritmo un leader che proporrà il valore finale. Per ricevere la ricompensa derivante dal proporre il blocco successivo i nodi devono dar prova di aver svolto un certo lavoro e possedere o una certa autorità o dei token. Questa tipologia consente un approccio completamente decentralizzato e consente di scalare facilmente soffrendo, però di lentezza di esecuzione.
- Meccanismi basati sulla tolleranza ai guasti convenzionali, al contrario dei precedenti richiedono bassa potenza computazionale e si affidano a un semplice schema di nodi che pubblica e verifica messaggi cifrati in un certo numero di fasi chiamate round. Una volta che un certo numero di messaggi è stato ricevuto nello

stesso round, si raggiunge un accordo. Questa tipologia è preferibile in blockchain private o con richiesta di permesso, con un numero di nodi limitato, poiché fornisce buone prestazioni, ma è difficilmente scalabile.

Di seguito descriveremo gli algoritmi di consenso più utilizzati e di maggior interesse per la nostra ricerca.

- Proof of work, prova di lavoro, richiede di provare un adeguato dispendio di risorse computazionali per poter proporre alla rete un valore eventualmente da accettare. Attualmente è l'unico algoritmo ad aver dato prova di efficacia contro qualsiasi attacco collusivo alla rete blockchain. Tra gli altri, è utilizzato da Bitcoin ed Ethereum.
- Proof of Stake, prova di quota partecipativa, si basa sul fatto che un nodo abbia un certo quantitativo di token investiti nella blockchain; quindi, il suo eventuale tentativo malevolo porti meno vantaggi di quelli di un corretto comportamento. In questo algoritmo è molto importante la variabile dell'età del gettone ovvero da quanto tempo le monete sono ferme nella blockchain, che insieme alla quantità detenuta, contribuisce a far aumentare la probabilità di essere selezionato per proporre il blocco e quindi guadagnarne la ricompensa. Attualmente è utilizzata da varie blockchain di nuova generazione come Cardano mentre Ethereum sta lavorando ad una transizione verso questo algoritmo.

2.6 Smart contracts

I contratti intelligenti o "smart contract" sono in estrema sintesi delle righe di codice implementate su una blockchain. A dispetto di questa semplice definizione essi hanno un grandissimo potenziale per migliorare e rivoluzionare vari campi della nostra esistenza, tutto questo grazie alle loro intrinseche proprietà:

- Eseguibili automaticamente, per la loro attivazione non è richiesto alcun intervento;
- Esecutivi, ogni condizione contrattuale viene eseguita automaticamente;
- Sicuri, in quanto eseguiti su blockchain che ne determina la resistenza alla manomissione;

- Deterministici, per ogni input producono sempre il corrispondente medesimo output;
- Semanticamente sensati, sono comprensibili sia agli umani che alle macchine;
- Inarrestabili, non vengono inferiti da alcun evento esterno. Una volta che le condizioni si sono verificate loro eseguiranno.

Il primo a teorizzare gli smart contract fu negli anni '90 Nick Szabo, un importante crittografo, la cui ricerca ha dato notevole spunto alla successiva creazione di bitcoin. Circa 20 anni dopo vi è la creazione della seconda blockchain, ethereum in cui grazie alla ethereum virtual machine e al "solidity" linguaggio di programmazione turing completo è stato possibile implementare la visione di Szabo. Nonostante il suo linguaggio di programmazione più limitato anche bitcoin è in grado di implementare elementari smart contract come "pagare x il giorno y". Sulle blockchain programmabili c.d. di seconda generazione attraverso gli smart contract è possibile costruire delle applicazioni decentralizzate che a loro volta compongono quello che è definita la terza versione della rete internet, il web3.0.

2.7 Oracoli

Gli smart contract essendo eseguiti su blockchain non hanno accesso ad alcuna informazione esterna ad essa in quanto sistema chiuso. In molti casi le condizioni di attivazione di uno smart contract provengono da eventi e dati esterni alla blockchain, i c.d. dati off-chain. Per andare incontro a questa esigenza sono stati sviluppati gli oracoli, delle interfacce che consentono agli smart contract di disporre di dati esterni in maniera sicura.

2.7.1 Il funzionamento di un oracolo

In primo luogo lo smart contract richiede i dati ad un oracolo. Quest'ultimo esegue la richiesta andando a ricercare e ad estrarre i dati dalla giusta fonte, per esempio, un database o un'altra blockchain. I dati ottenuti vengono inviati ad un notaio virtuale per generare una prova crittografica, generalmente una firma digitale, per provare la validità ed autenticità dei dati, che vengono quindi inviati all'oracolo. I dati autenticati possono essere salvati su un servizio di archiviazione decentralizzato come Swarm o IPFS ed essere eventualmente utilizzati dalla blockchain o dallo smart contract per ulteriori verifiche. Questo procedimento opzionale è utile specialmente nel caso in cui vi siano grandi quantità di dati autenticati e

archiviarli sulla blockchain risulterebbe infattibile. Infine i dati autenticati crittograficamente sono inviati allo smart contract.

2.7.2 Prova di autenticità

Per motivi di sicurezza gli oracoli devono essere in grado di firmare digitalmente i dati e questa prova è definita “proof of authenticity” prova di autenticità. Gli smart contract una volta iscritti ad un oracolo possono sia richiedere le informazioni che direttamente riceverle da esso. Gli oracoli sono tenuti a fornire dati reali e devono essere impossibilitati alla loro modifica poiché nonostante la loro prova di autenticità potrebbe accadere che in alcuni casi i dati siano corretti a causa di manipolazioni o di errori di sistema. La prova di autenticità può essere raggiunta crittograficamente in vari modi:

- Prova fornita da software o dalla rete, questa tipologia di prove si affida a protocolli di network, a software o ad una combinazione di entrambi. Di seguito i metodi più utilizzati:
    - TLSNotary, un protocollo che fornisce una prova inconfutabile del fatto che sia avvenuta una comunicazione tra un client ed un server. Si basa su uno standard di sicurezza, TLS “Transport Layer Security” ovvero strato di trasporto in sicurezza, che consente una comunicazione bidirezionale sicura tra gli host che grazie alla sua efficacia è ampiamente utilizzato anche per rendere sicuri i siti internet. Per provare l'autenticità dei dati procurati dagli oracoli su fonti esterne è utilizzato il meccanismo di attestazione TLS Notary che produce una prova verificabile della comunicazione avvenuta tra la fonte e l’oracolo. Questa prova di autenticità assicura che i dati mandati allo smart contract siano stati effettivamente recuperati da quella fonte;
    - Meccanismo basato su TLS-N, consiste in una estensione del sopra descritto TLS dotandolo di sicure garanzie di non ripudiabilità. Consente di creare la prova non interattiva di un determinato contenuto ricevuto da una sessione di trasporto sicura TLS preservando la riservatezza. Gli oracoli basati su questa tecnologia non hanno bisogno di affidarsi ad hardware di terze parti per provare l’autenticità dei dati estratti dalla rete internet forniti alla blockchain. Questa tecnologia consente una

decentralizzazione della verifica delle informazioni estratte e trasportate dagli oracoli da internet ad una blockchain;

- Prova fornita da dispositivo, consente di utilizzare parti di hardware per verificare l'autenticità dei dati. Di seguito sono elencati i maggiormente utilizzati:
    - Android, la tecnologia “SafetyNet” Android di verifica software e hardware consente di ottenere un dispositivo comprovatamente sicuro e verificabile. SafetyNet si occupa di assicurarsi che una applicazione Android sia eseguita su un dispositivo sicuro e non manomesso su cui operi l’ultima versione del sistema operativo in modo da prevenire ogni tipo di sfruttamento delle vulnerabilità conosciute nelle versioni precedenti. Il dispositivo reso sicuro grazie a questi meccanismi viene utilizzato per estrarre i dati da fonti di terze parti assicurando una connessione sicura a prova di manomissione, consentendo quindi di comprovare l’autenticità dei dati estratti;
    - Ledger, attraverso i suoi dispositivi per custodire e scambiare criptovalute in modo sicuro, i c.d. “hardware wallet”, consente di servirsi del loro particolare sistema operativo chiamato “Blockchain open ledger operating system" che garantisce a livello dispositivo e di programmazione un ambiente sicuro che può essere utilizzato per sviluppare varie applicazioni come quella di gestione delle criptovalute. Queste caratteristiche consentiranno quindi alle applicazioni sviluppate dagli Oracoli su questi dispositivi di essere eseguite su un ambiente comprovatamente sicuro e quindi di avere una “proof of authenticity”;
    - Prova fornita da hardware fidati, come quelli garantiti da TEE “Trusted Execution Environment” ovvero ambiente fidato di esecuzione, una parte del processore principale di un dispositivo, che garantisce confidenzialità ed integrità ai dati ed al codice in esso inseriti con meno funzionalità di un sistema operativo ma con molta più sicurezza.

2.7.3 Tipologie di oracoli

Ecco una lista di alcune tipologie di oracoli che possiamo trovare nelle architetture della blockchain:

- Oracoli in entrata, macro-tipologia che include tutti quelli che ricercano ed inviano dati da fonti esterne agli smart contract. Di seguito alcuni esempi:
    - Software, chiamati anche oracoli semplici o standard, acquisiscono informazioni dal web e sono utilizzati principalmente per ottenere dati dai mercati finanziari, previsioni meteorologiche ed altre informazioni fornite da terze parti.
    - Hardware, acquisiscono informazioni da dispositivi fisici collegati alla rete, c.d dispositivi "IoT" Internet of things, o sensori. Sono utilizzati in contesti in cui sia necessario monitorare il comportamento di un determinato oggetto nel mondo reale come, per esempio, una automobile assicurata attraverso smart contract. Questi oracoli necessitano di affidarsi ad hardware sicuri e non manomissibili che attualmente sono tutelati da crittografia e meccanismi antimanomissione che li renderebbero inutilizzabili al primo tentativo di alterazione.
    - Computazionali, consentono di esternalizzare calcoli onerosi per poi riportarli on-chain, garantendo integrità e autenticità.
    - Basati su aggregazione di dati, ricercano su differenti fonti lo stesso dato ed a seconda della necessità ne traggono una media una mediana ecc. che inviano allo smart contract. La sicurezza di questi oracoli è basata sul fatto che elaborando una moltitudine di fonti consultate per lo stesso dato si riesca ad ottenere una informazione affidabile.
    - Guidati dalla c.d. saggezza della folla, un altro metodo insieme al precedente con cui si può superare la sfiducia nell'affidarsi ad una singola risorsa. Vengono confrontate varie fonti pubbliche come news e gente comune, per ottenere una vasta mole di informazioni sullo stesso dato da cui, se ottenuto molte volte lo stesso risultato sarà altamente probabile che questo sia corretto ed affidabile.
    - Decentralizzati o guidati dal consenso, sono nati dalla necessità di affrontare il problema della fiducia negli oracoli (di cui tratteremo a breve), e si basano sul consenso distribuito. Questi oracoli possono prelevare dati da altre blockchain per cui quindi non sono necessarie terze parti a garanzia oppure possono raccogliere dati off-chain attraverso algoritmi di incentivo e disincentivo basati sulla teoria della saggezza della

folla in cui ogni operatore partecipante comunica all'oracolo decentralizzato la propria versione di una determinata informazione.

- Oracoli smart, sono dei normali oracoli di una qualsiasi delle precedenti categorie con la caratteristica di poter eseguire a loro volta delle righe di codice utilizzando ambienti chiusi di programmazione ed esecuzione.

- Oracoli in uscita o Oracoli invertiti, nascono dalla necessità di portare dati dalla blockchain all'esterno. Le destinazioni possono essere altre blockchain, dei dispositivi che vengono attivati da determinate informazioni provenienti dalla blockchain per aggiungere un ulteriore grado di sicurezza o dei database aziendali;

2.7.4 Il problema della fiducia negli oracoli

Gli oracoli portano dati esterni agli smart contract sulla blockchain, questo processo comporta un contrasto tra la blockchain che non ha bisogno di affidarsi a nessuno e gli oracoli che per funzionare attualmente devono fidarsi di terze parti. La maggior parte degli smart contract necessitano di oracoli questo però compromette la loro decentralizzazione poiché nonostante si operi su una blockchain pubblica il risultato del contratto dipende fortemente dai dati forniti dall'oracolo. Ipotizzando di porre la fiducia in un organismo centrale questo potrà comunque essere manovrato da legislazioni , da pressioni socio-economiche e da attacchi informatici fornendo dati inesatti all'oracolo che a sua volta potrebbe incappare in malfunzionamenti interni, guasti e attacchi informatici.

3. L'APPLICAZIONE DELLA BLOCKCHAIN AL MERCATO DEGLI EVENTI DAL VIVO

3.1 Proposte e riflessioni

La tecnologia blockchain negli ultimi anni è entrata a far parte di molti ambiti della nostra esistenza soprattutto per ora a livello teorico accademico, ma non esita ad avere le sue implementazioni ormai degne di nota. Oltre a finanza, gestione di dati sanitari, diritto d'autore, un'applicazione attualmente su cui si concentrano molti investimenti è quella della gestione efficace e trasparente di filiera. Quella della vendita e della eventuale rivendita di biglietti può essere considerata tale a tutti gli effetti.

Nell'esame delle problematiche riguardanti il mercato secondario di biglietti ne sono emerse principalmente tre:

1. contraffazione dei biglietti,
2. speculazione di agenti esterni che senza aggiungere valore al settore ne traggono del profitto,
3. utilizzo più o meno illecito di varie identità per l'acquisto da parte di un singolo ente di notevoli quantità di biglietti sul primario da rivendere sul secondario.

Di seguito si è provato a speculare sulla risoluzione delle suddette questioni:

1. Il problema della contraffazione, creando i biglietti su blockchain come token non fungibili, è facilmente risolvibile affidandosi esclusivamente alla tecnologia. Ogni postazione del luogo di un evento ha una sua unicità, magari dovuta anche solo ad una leggera differenza di inclinazione del volto necessaria a guardare il palco o la sua distanza dall'uscita o dai servizi, proprio per questo si presta moltissimo ad essere emesso in blockchain direttamente come token non fungibile.
2. Una particolarità degli "NFT" è quella di poter inserire in essi uno smart contract che per ogni transazione devolve una percentuale predeterminata del margine ottenuto a colui che ha inserito in blockchain il token ed eventualmente ad altri scelti da quest'ultimo. Questo consente agli agenti primari di ricavare dei guadagni dalle speculazioni effettuate da agenti esterni parassiti o da malevoli colleghi. Si tutela inoltre la reputazione di quegli artisti che per varie motivazioni vogliono imporre prezzi inferiori all'incrocio di mercato.

3. La questione dell'acquisto sul primario mediate multiple identità è attualmente aggirabile mediante il ricorso ad aggressive procedure di "KYC" know your customer, conosci il tuo cliente, in cui si richiede all'utente di registrarsi alla piattaforma inserendo dati personali e biometrici attraverso i quali garantire la propria identità e proattività nell'effettuare l'acquisto. Questa soluzione è in netto contrasto con la filosofia blockchain di disintermediazione e decentralizzazione, ma consente di arginare considerevolmente il problema. Affidandosi ad una apposita autorità di vigilanza si potrà controllare se delle persone, soprattutto se collegate ad agenti primari, stiano acquistando biglietti e monitorare i loro comportamenti per smascherare eventuali schemi di acquisto speculativo sia privati che di gruppo. Grazie al riconoscimento biometrico dinamico per effettuare la compravendita sarà possibile accertare che questa sia effettuata dall'utente in prima persona e non solo attraverso i suoi dati e la sua carta di credito e con lo svilupparsi della tecnologia si potrà anche garantire che l'acquisto non stia avvenendo sotto coercizione.

Date queste premesse si può prevedere una speculazione dilettantistica a livello di singolo consumatore o in organizzazioni ma sicuramente limitata in quantità e frequenza. Nel caso in cui da una parte l'avidità fosse tale da rendere indisponibili i biglietti accessibili ai redditi più bassi , appositamente emessi da agenti primari sensibili alla causa, dall'altra sicuramente si andrebbero a creare organizzazioni senza scopo di lucro per riappropriarsi dei biglietti e proporli a prezzi magari anche più bassi del nominale ad individui certificatamente meritevoli.

3.2 Revisione della letteratura

3.2.1 TickEth

Ricercando nella attuale letteratura riscontriamo vari tentativi ed approcci alla vendita di biglietti attraverso blockchain. Uno di questi è sicuramente TickEth, progetto che nasce dalla volontà di risolvere la duplicabilità e contraffazione dei biglietti venduti online, i margini spropositati applicati dai rivenditori e la difficoltà delle procedure di rimborso. Come auspicabile dal nome la piattaforma ospitante di questa applicazione decentralizzata

sarà Ethereum, blockchain pubblica, prima ad aver sviluppato la possibilità di implementare smart contract.
Ecco illustrato il suo funzionamento. L'utente per iniziare ad operare deve registrarsi ad un server centrale per garantire l'assenza di bot dalla piattaforma. L'autenticazione avverrà mediante scansione di documenti e l'accertamento del possesso di un indirizzo ethereum, ovvero un wallet. Ogni persona potrà avere associato al massimo un indirizzo valido contemporaneamente. In un secondo momento l'indirizzo ethereum verrà inserito su uno smart contract ma non sarà mai reso pubblico sulla blockchain. L'indirizzo validato potrà dunque vendere e comprare sulla piattaforma attraverso smart contract.
Per l'acquisto di biglietti uno smart contract creato appositamente per l'evento si occuperà di vendita ed eventuale rivendita di biglietti sia ad utenti che interagiscono direttamente su ethereum sia a coloro che utilizzeranno altre interfacce. Il contratto conterrà tutte le informazioni relative come nome e descrizione dell'evento; quantità, prezzo, tipologia, finestra temporale di vendita, numero massimo acquistabile per singolo indirizzo. Una volta attivata la funzione "acquista" verranno effettuate le seguenti verifiche:

- Validità dell'indirizzo dell'acquirente, ovvero la sua presenza nel database dello smart contract degli indirizzi validati.
- Validità della finestra di acquisto.
- Disponibilità di posti.
- Disponibilità di valuta, ETH da parte dell'acquirente.

Se non sarà superata la verifica i fondi saranno inviati all'indirizzo ethereum mentre se andrà a buon fine il contratto dell'evento salverà tutti i dettagli della transazione.

La fase dell'accesso all'evento ha posto i ricercatori di fronte alle seguenti limitazioni:

- Lentezza intrinseca di una blockchain in Proof of work, quindi impossibilità di annullare i biglietti già utilizzati;
- Potrebbe essere problematico e non sempre possibile un accesso costante alla rete internet e gli spettatori potrebbero essere impossibilitati ad utilizzare il proprio telefono magari perché scarico.

Si è quindi deciso di affidarsi ad una soluzione che non necessiti di connessione e che consenta anche l'utilizzo del cartaceo.

Terminato il periodo di vendita le informazioni vengono inviate ad un database server, che consentirà ai dispositivi di controllo delle entrate all'evento di verificare la validità dei biglietti e tenere traccia di quelli già utilizzati. I ricercatori ammettono che però questo non consentirebbe di vendere direttamente sul luogo dell'evento, ma aggirano l'ostacolo lasciando che una ultima frazione dei biglietti sia tenuta da parte per essere venduta nel luogo dell'evento, considerato che in questo modo non vi è pericolo di manipolazioni, truffe o speculazioni. Il possessore del titolo avrà come prova un QR-code contenente la garanzia crittografica che verrà validata da un apposito dispositivo atto anche ad aggiornare le informazioni nel database.

Per quanto riguarda il mercato secondario invece, per vendere dei biglietti è necessario comunicarne allo smart contract adibito identificazione crittografica, quantità e prezzo, che per evitare speculazioni dovrà essere ristretto ad un determinato intervallo determinato a monte nella creazione dello smart contract per conto degli attori coinvolti nell'organizzazione dell'evento. Chi volesse acquistare sul secondario ha la possibilità di farlo specificando allo smart contract apposito evento, identificatore vecchio possessore e del nuovo, inoltrando infine la quantità di ETH richiesta. La transazione sarà accettata se:

- gli identificatori dei biglietti corrispondono a quelli messi in vendita per quel determinato evento
- gli ETH inviati corrispondano al prezzo indicato dal rivenditore
- vi è corrispondenza tra la quantità di biglietti venduti e quelli acquistati
- gli identificativi dei nuovi biglietti sono diversi da quelli appena venduti e da quelli ancora disponibili

Per quanto riguarda i rimborsi invece, allo stato attuale dell'arte ricevere un rimborso anche per validi motivi da parte dell'emittente risulta molto macchinoso. Nel caso di questo sistema di distribuzione, grazie alla blockchain, appena un evento sia annullato dall'organizzazione, gli indirizzi acquirenti saranno rimborsati quasi automaticamente dallo smart contract. Gli organizzatori possono decidere anche se trattenere una percentuale di gestione, differente anche in base alla tipologia di acquirente.

Ecco alcune politiche a difesa della riservatezza: nella blockchain pubblica di Ethereum non verrà mai esplicitato il nome dell'acquirente ma solo una stringa alfanumerica identificativa del portafoglio digitale. Nel caso in cui l'indirizzo venga associato sia in buona che in cattiva fede ai dati del suo possessore, chiunque potrà tracciarne e verificarne le transazioni passate e future. Prima o poi questo potrebbe creare dei problemi quindi si è pensato di implementare una procedura per il cambio di indirizzo. L'utente richiede al server centrale di poter

cambiare indirizzo indicando vecchio e nuovo. Il nuovo indirizzo è validato dallo stesso smart contract che valuta in fase di registrazione. L'utente sarà poi chiamato a svolgere delle operazioni richieste dallo smart contract validatore per garantire la proprietà dell'indirizzo. Effettuate tutte le verifiche il vecchio indirizzo sarà sostituito dal nuovo.
Una ulteriore tutela per il consumatore è data dal fatto che il nuovo indirizzo è inserito in blockchain con un ritardo casuale in modo da impossibilitare la correlazione tra i due indirizzi leggendo lo storico della blockchain.
Esisteranno poi dei rivenditori autorizzati. Gli organizzatori che volessero delegare la rivendita dei propri biglietti hanno la possibilità di farlo creando uno smart contract dedicato ed inserendo il suo indirizzo tra quelli autorizzati. Potrà essere liberamente decisa una percentuale di prestazione da devolvere al rivenditore e gli acquirenti attraverso la propria interfaccia potranno acquistare da chi riterranno più opportuno utilizzando il proprio indirizzo e interpellando la funzione "compra" dello smart contract.

3.2.2 Un'implementazione alternativa

Nel libro "Blockchain Technology: Applications and Challenges" di Sandeep Kumar Panda, Ajay Kumar Jena, Santosh Kumar Swain e Suresh Chandra Satapathy si teorizza una possibile implementazione di una piattaforma di vendita di biglietti online basata su blockchain. Le parti coinvolte nell'ecosistema e le loro funzioni sono le seguenti:

- amministratore, entità che provvede alla creazione di una piattaforma sulla rete che consenta la registrazione per l'evento e che invii i token alla organizzazione preposta. Gli amministratori chiuderanno un accordo con gli organizzatori disponibili ad organizzare l'evento;
- organizzatore, si occuperà di pianificare e gestire la realizzazione dell'evento tenendo sempre informato l'amministratore che dovrà costantemente aggiornare l'interfaccia di acquisto dell'utente;
- evento, insieme di tutte quelle informazioni come descrizione, data, luogo, tipologia e prezzi dei vari posti;
- utenti, coloro che vorranno partecipare all'evento. Questi dovranno registrarsi attraverso il sito provvisto dagli amministratori, fornendo i loro dettagli come generalità, numero di telefono e posta elettronica. Successivamente potranno scambiare denaro fiat per la rispettiva quantità di token che verranno depositati in un portafoglio di criptovalute fornito dagli amministratori in fase di registrazione;

- token, denaro virtuale con la caratteristica di rendere possibile il trasferimento di proprietà dei biglietti;
- biglietto, sotto forma anche questa volta di QR-code generato partendo da identità dell'acquirente e dettagli dell'evento e sarà inviato a ridosso dell'inizio dell'evento per evitare che possa essere contraffatto. Il QR-code dovrà poi essere scannerizzato all'entrata per verificarne il merito di ingresso all'evento.

REGISTRAZIONE

L'utente sarà tenuto a fornire nome generalità e dettagli di contatto e gli verrà creato l'account sulla piattaforma. Successivamente verrà inviato un OTP ad uno dei contatti registrati dall'utente che dovrà usarlo per accedere per la prima volta e creare la sua password. Alla fine di tutto questo l'account sarà ufficialmente creato.

PAGAMENTO

Gli interessati all'acquisto dovranno inviare un determinato importo di denaro Fiat agli organizzatori che creeranno il token corrispondente in blockchain e lo invieranno al wallet dell'utente. Ricevuti i token l'utente potrà effettuare l'acquisto e se valido riceverà un messaggio di conferma.

SMART CONTRACT

nella ricerca di cui ora stiamo parlando sono stati implementati tre smart contract concatenati tra loro uno dopo l'altro:

1. Il contratto di registrazione utente, creato dagli amministratori, consente la funzione di registrazione degli utenti e consente di conservare le loro informazioni per sempre. L'utente dovrà fornire i suoi dati identificativi e di contatto e riceverà un codice univoco sul suo numero di telefono attraverso cui finalizzare la registrazione. Subito dopo lo smart contract svilupperà il portafoglio digitale con l'indirizzo dell'utente corrispondente e lo assegnerà ad esso.
2. Contratto di creazione portafoglio digitale, sviluppato dall'utente dopo la registrazione. Il portafoglio creato conterrà un token con valore zero. Attraverso una funzione dedicata il valore del token potrà essere aumentato attraverso pagamenti verificati in denaro. Un'altra funzione garantirà di assegnare e aggiornare la proprietà dei biglietti.
3. Contratto di aggiornamento del biglietto, è attivato non appena verificato l'acquisto del token e consente le funzioni di "compra biglietto" che svuoterà del valore corrispondente il token del portafoglio dell'utente, e di "aggiorna biglietto"

che fornisce informazioni sul proprietario effettivo del biglietto. Al primo acquisto il QR-code verrà immediatamente rilasciato altrimenti verrà riferito l'hash della transazione precedente. La transazione con tutte le relative informazioni come hash dell'attuale acquirente, il venditore, l'hash della precedente transazione ed la sua firma temporale "timestamp", sarà inserita nella lista di quelle elaborate in questo contratto. Se la transazione corrente sarà correttamente ultimata, verrà modificato l'elenco delle transazioni precedenti con la sua aggiunta e sarà aggiunta alla blockchain solo se l'hash della precedente transazione è valido. Questo consente di garantire che ogni transazione aggiunta al blocco sia lecita e veritiera, inibendo di fatto la vendita di falsi biglietti o la vendita dello stesso biglietto più volte.

CONCLUSIONE

Lo scopo di questo elaborato è proporre una soluzione innovativa, che sfrutta le tecnologie della blockchain, per risolvere un problema che esiste dalla nascita dei primi eventi dal vivo.

La tecnologia blockchain negli ultimi anni è entrata a far parte di molti ambiti della nostra esistenza soprattutto per ora a livello teorico accademico, ma non esita ad avere le sue implementazioni ormai degne di nota. Oltre a finanza, gestione di dati sanitari, diritto d'autore, un'applicazione attualmente su cui si concentrano molti investimenti è quella della gestione efficace e trasparente della filiera. Quella della vendita e della eventuale rivendita di biglietti può essere considerata tale a tutti gli effetti. Da quanto emerso dalla nostra analisi, sia TickEth, progetto che nasce dalla volontà di risolvere la duplicabilità e contraffazione dei biglietti venduti online, che la teoria sviluppata in "Blockchain Technology: Applications and Challenges" sono progetti interessanti che provano a dare risposte alle lacune del mercato del ticketing.

Come analizzato le soluzioni sembrano essere tutte valide, ma ognuna di esse sembra presentare un suo specifico punto di debolezza: un eccessivo ed invasivo controllo personale, che invade quasi l'integrità individuale, l'affidarsi ad un server centrale o ad un'istituzione centralizzata. Il progresso tecnologico che si verificherà nei prossimi anni consentirà sicuramente di risolvere i problemi, come il secondary ticketing, che affliggono l'industria degli eventi dal vivo e della musica, ma serviranno ancora ulteriori innovazioni ed applicazioni nel settore. Quello degli eventi dal vivo rimarrà certamente un mercato florido per le aziende emergenti del 2022 che dovranno farsi trovare pronte per la riapertura completa e quindi la ripresa degli eventi dal vivo dopo l'auspicabile fine dell'emergenza Covid-19.

BIBLIOGRAFIA

- Almasoud, A. Eljazzar, M.M. Hussain, F. *Toward a self-learned Smart Contracts*. IEEE Xplore, 2018;
- Bashir, I. *Mastering Blockchain*. Packt Publishing, 2020;
- Campbell, R. *BitTicket Uses Ethereum Classic to Book Tickets on a Blockchain*. Archive, Capital & Crypto, 2017;
- Corsi, P. Lagorio, G. Ribaudo, M. *TickEth, a Ticketing System built on Ethereum*. Symposium on Applied Computing, 2019;
- Cyrenne, P. *Antiscalping laws and the selling of season tickets by professional sport teams*. John Wiley & Sons, Ltd, 2019;
- Dong-Hyun, K. Hyung-Kwang, C. Kil-Sub, K. *A Design and Implementation of Macro Prevention Ticket Booking System Using Blockchain*. The 6th International Conference on E-Business and Applications, 2020;
- Drayer , J. *Examining the effectiveness of anti-scalping laws in a United States market*. Sport Management Review, 2011;
- Drayer , J. *Making a case for the integration of the primary and secondary ticket markets for professional team sports in the United States.* International Journal of Sports Marketing & Sponsorship, 2011;
- Hu, K. Zhu, J. Ding, Y. Bai, X. Huang, J. *Smart Contract Engineering*. Electronics, 2020;
- Idrees, S.M. Aijaz, I. Jameel, R. Nowostawski, M. *Exploring the Blockchain Technology Issues, Applications and Research Potential*. International Journal of Online and Biomedical Engineering, 2021.
- Krueger, A.B. *Rockonomics*. John Murray, 2019;
- Levi, S.D. Lipton, A.B. *An Introduction to Smart Contracts and Their Potential and Inherent Limitations.* Skadden, Arps, Slate, Meagher & Flom LLP, 2018.
- Li, X. Niu, J. Gao, J. Han, J. *Secure Electronic Ticketing System based on Consortium Blockchain*. KSII Transactions on Internet and Information Systems (TIIS), 2019;
- Prisco, F. *Music Economy*. Allegato a Il Sole 24 Ore, 2019;
- Quiniou, M. *Blockchain: the advent of disintermediation*. John Wiley & Sons, Ltd, 2019;
- Ritzdorf, H. Wüst, K. Gervais, A. Felley, G. Capkun, S. *TLS-N: Non-repudiation over TLS Enabling Ubiquitous Content Signing for Disintermediation*. Department of Computer Science, ETH Zurich, 2017;
- Rushton, I. *Touts out? The Waterson review on secondary ticketing.* Routledge, 2016;
- Sohee, K. Sejun, Y. Nagarajan, R. Nguyen-Truong, L. Hyunseok, P. *Developmental trajectories of blockchain research and its major subfields*. IEEE Access, 2020;
- Vihas, N. Shanmukhi, P.D. Shagun, S.L., Varaprasad, R. *Blockchain Technology: Applications and Challenges*. Intelligent Systems Reference Library, 2021;
- Waterson, M. *Independent Review of Consumer Protection Measures concerning Online Secondary Ticketing Facilities.* Crown copyright, 2016;
- Whitaker, A. *Art and Blockchain: A Primer, History, and Taxonomy of Blockchain Use Cases in the Arts*. ARTIVATE, 2019.