

POLITECNICO DI TORINO



Facoltà di Ingegneria

Corso di Laurea Magistrale in Ingegneria Gestionale

Analisi economica e tecnica di applicazioni basate sulla
tecnologia blockchain

Relatore Prof. Marco Torchiano

Candidato Marta Chiatello

s238166

Indice

Introduzione	3
1. Blockchain	5
1.1 Transazioni.....	7
1.2 Mining.....	8
1.3 Utenti	9
1.4 Elementi distintivi della blockchain.....	10
Sicurezza e crittografia.....	10
Fiducia o Trust	13
Altre caratteristiche	13
1.5 Token	13
1.6 Ambiti di utilizzo	14
Smart Contract e Ethereum	15
Altri ambiti.....	17
Nota sulla nomenclatura.....	17
2. Criptovalute e Bitcoin	18
2.1 Mining.....	18
2.2 Double Spending.....	21
2.3 Bitcoin.....	22
2.4 Ethereum ETH	23
2.5 Ripple XRP	24
2.6 Bitcoin Cash BCH.....	24
2.7 Litecoin LTC.....	25
2.8 Dash DASH	25
2.9 Iota IOT.....	25
2.10 Nem XEM.....	26
3. Card.....	27
3.1 Gift Card	27
Cos'è e come funziona	27
Vantaggi.....	28
Problemi associati all'utilizzo e limiti delle gift card	29

Welfare aziendale.....	29
3.2 Loyalty Card	30
Cos'è e come funziona	30
Vantaggi.....	31
Problemi associati	31
4. Studi di applicazione della blockchain alle gift card e loyalty card.....	32
4.1 Dati e statistiche sulle loyalty card	32
4.2 Ruolo della tecnologia blockchain.....	33
5. Le realtà presenti sul mercato: casi di studio	36
5.1 BitRewards.....	36
Funzionamento.....	36
Meccanismo di reward.....	37
Pagamento di acquisti tramite l'operatore BitRewards	37
Mantenimento delle riserve fiat e criptovalute presso l'operatore BitRewards.....	38
Smart Contract di liquidità.....	38
Architettura di prodotto.....	39
5.2 QiiBee	41
Vantaggi per il brand	41
Vantaggi per i clienti.....	41
Funzionamento.....	42
LoyaltyToken Protocol	43
5.3 Tokky	44
Funzionamento.....	45
Architettura di prodotto.....	47
5.4 Zeex	48
Implementazione.....	49
5.5 Particolarità del mercato italiano	51
Intervista al CIO di Amilon	53
Conclusioni	56
Bibliografia e Sitografia.....	59

Introduzione

Negli ultimi mesi l'attenzione mondiale è ricaduta sulla blockchain e sul mondo delle criptomonete, che, nonostante siano in uso già da qualche anno, hanno però suscitato notevole interesse anche ai non addetti ai lavori, tanto che è sempre più frequente trovare articoli di quotidiani o giornali online non specializzati che trattano l'argomento. Quando ho iniziato a informarmi su questa tecnologia in modo più sistematico e organizzato, era l'inverno del 2017 e Bitcoin sembrava la parola del momento: si stavano, infatti, verificando oscillazioni notevoli del suo valore; si andava configurando una nuova struttura e il Bitcoin era visto come una sorta di spartiacque finanziario all'interno di un sistema mondiale in transizione. Per la prima volta, un prodotto stava concentrando a poli opposti le previsioni di mercato, ma soprattutto per la prima volta un prodotto era indefinibile.

In poco tempo, la Bitcoin - mania coinvolge anche la tecnologia che sta alla base della criptovaluta più famosa al mondo e così l'interesse si allarga anche alla comprensione della Blockchain per analizzarne il funzionamento, ma soprattutto per studiarne le caratteristiche con l'obiettivo di implementare questa innovazione anche in molteplici settori differenti tra loro. E così se in un primo momento il duo Blockchain - Bitcoin veniva associato solamente al mondo finanziario, ben presto si è iniziato ad accostare la blockchain ad ambiti quali la pubblica amministrazione, la logistica, il sistema di votazione, le soluzioni per smart cities e così via.

Questa tesi di laurea mira ad analizzare dal punto di vista tecnico ed economico l'utilizzo della blockchain nell'ambito delle gift card e loyalty card. L'obiettivo è capire se sia davvero possibile implementare la nuova tecnologia con questo particolare scopo, se sia già in uso o si preveda nel breve periodo di lanciarla sul mercato e soprattutto se apporterà vantaggi rispetto alla situazione attuale.

Per fare ciò è stato innanzitutto fondamentale studiare in modo imparziale la blockchain, evitando giudizi e pregiudizi al fine di scongiurare l'ipotesi di propendere dalla parte di chi esalta eccessivamente questa tecnologia, ma neanche dalla parte di chi la scredita in quanto poco significativa. Il primo capitolo, quindi, presenta una descrizione sufficientemente tecnica per comprendere il meccanismo di funzionamento e le caratteristiche che la rendono così particolare e interessante. Poiché è impossibile parlare di blockchain senza menzionare le criptovalute, il secondo capitolo è dedicato ad un approfondimento delle monete digitali, partendo dal loro funzionamento per arrivare a una rapida panoramica sulle valute più famose e utilizzate nel mondo online.

Il terzo capitolo entra più nello specifico, in quanto è la descrizione delle card: che siano gift o loyalty, in comune hanno la caratteristica di essere strumenti legati al

marketing aziendale; qui è spiegato il loro funzionamento con un occhio al contesto italiano, non sempre paragonabile a ciò che si verifica a livello mondiale, dove la diffusione è ovviamente più ampia.

Successivamente, con il quarto capitolo si entra nel vivo dell'analisi perché viene affrontato uno studio condotto da Deloitte in merito all'applicabilità della blockchain nel mondo loyalty; le numerose informazioni e statistiche contenute a inizio capitolo permettono di comprendere l'utilizzo delle gift card e delle loyalty card per quanto riguarda le abitudini dei consumatori e i comportamenti d'acquisto della clientela.

Infine, la parte più approfondita della tesi è costituita dal quinto capitolo che ha lo scopo di presentare quattro piattaforme esistenti: due rientrano nell'ambito delle carte fedeltà, mentre le restanti in quello delle carte regalo. Per ciascuna, è descritto il funzionamento con un focus su come è implementata la blockchain. A completare questa esposizione, è riportato il contenuto di un'intervista condotta a un professionista italiano del settore, che, per quanto riguarda l'applicazione della blockchain nei due ambiti in questione, ha espresso il suo personale parere cui è giunto in seguito a una verifica di fattibilità svolta all'interno della propria società. Per ultime, le conclusioni riportano un breve riassunto di ciò che è emerso nel corso della stesura della tesi tenendo conto delle innovazioni già presentate sul mercato o in fase di lancio e dell'opinione di chi lavora a diretto contatto con la tecnologia blockchain e sa discernere l'utilità dal trend del momento.

CAPITOLO 1

1. Blockchain

Negli ultimi mesi le notizie di carattere tecnologico e finanziario riportavano la stessa *buzzword*: Blockchain.

Come ogni novità, è associata a curiosità ma anche a interrogativi circa la sua efficacia e reale applicazione. Per molti, la blockchain è una nuova generazione di Internet, una tecnologia che pone l'attenzione sulle Transazioni e sul Valore. Si può affermare che sia la rappresentazione di quattro concetti forti e ben distinti: decentralizzazione, trasparenza, sicurezza e immutabilità. Inoltre, ingloba un concetto di Trust che automaticamente avvicina la blockchain a una connotazione più politica, secondo cui è possibile una piattaforma che permette lo sviluppo di una nuova forma di democrazia.

Inizialmente, la blockchain è stata confusa e identificata con i Bitcoin, ovvero con quella parte di blockchain che sta alla base delle *digital currency* o criptomonete. Questo perché lo scenario in cui si è sviluppata la blockchain è legata inesorabilmente a quello economico-finanziario.

Nel corso dei secoli, infatti, sono stati introdotti strumenti di fiducia come monete, contanti, lettere di credito e vari sistemi bancari con lo scopo di facilitare transazioni e al tempo stesso proteggere venditori e compratori. Negli ultimi decenni, grazie ad innumerevoli innovazioni, tra le quali spicca l'impiego di Internet, si è decisamente ridotta la distanza tra chi voleva vendere e chi acquistare e, di conseguenza, il desiderio comune è stato quello di permettere rapidità, convenienza e efficienza alle transazioni. In un contesto frenetico e ampiamente collegato come quello odierno, il volume delle transazioni cresce esponenzialmente e richiede sempre più una rete caratterizzata da velocità, affidabilità, accessibilità e sicurezza per garantire la continuità degli scambi. Proprio per questi motivi, nel 2009 è stata rilasciata da un anonimo, noto con lo pseudonimo di Satoshi Nakamoto, una nuova tecnologia da applicare in quest'ottica: la blockchain.

Una prima definizione di blockchain la descrive come un archivio permanente che memorizza e gestisce transazioni; queste vengono immagazzinate in blocchi solo dopo che la rete stessa ha approvato e verificato la correttezza delle informazioni, di conseguenza ciascun blocco è contemporaneamente archivio e controllore di tutte le transazioni. Il fatto che tutti i partecipanti della rete siano collegati tra loro permette la tracciabilità e garantisce l'immutabilità delle transazioni avvenute, e ciò anche grazie all'utilizzo di sistemi di crittografia a difesa della sicurezza.

Al tempo stesso, una seconda interpretazione della blockchain è quella di registro pubblico del tipo DLT (Distributed Ledger Technology), ovvero *Libro Mastro distribuito* in quanto non esiste più il concetto di sistema centralizzato caratterizzato dall'autorevolezza del soggetto al centro dell'organizzazione, bensì una nuova logica in cui tutti i membri sono di pari livello e in cui si instaura un rapporto di fiducia tra essi. Si tratta quindi di una rete *peer-to-peer* in cui vengono registrate le transazioni e i dati di chi le esegue.

Alla base dei DLT c'è il concetto di grandi network costituiti da una serie di partecipanti, detti nodi; ognuno è autorizzato ad aggiornare i ledger in modo indipendente dagli altri, ma sotto la *regola del consenso*. Questo significa che ogni nodo crea e carica autonomamente dati da registrare sulla rete, ma non prima che gli altri nodi abbiano verificato, votato e approvato (in maggioranza) la transazione in questione.

I *ledger* non sono una novità; vengono usati fin dal XIII secolo nella contabilità in partita doppia e nell'archiviazione di dati e transazioni contabili. L'utilizzo dei Libri Mastro da parte delle Pubbliche Amministrazioni ha sempre permesso di conoscere e verificare in qualunque momento i dati relativi a un asset e al suo proprietario; chiaramente alla base di questo sistema era necessaria la fiducia nel sistema centrale che gestiva l'accesso e l'utilizzo del Ledger. Ciò che è innovativo con la blockchain è il concetto di Libro Mastro distribuito e condiviso (Figura 1), ovvero un registro immutabile contenente tutte le transazioni avvenute in un certo network e a cui possono accedere, in modo molto rapido, tutti i partecipanti del network stesso, grazie al fatto che il database non si trova fisicamente su un solo server, ma su tutti i computer partecipanti alla rete. Non è più necessario fare riferimento a una struttura centrale e, di conseguenza, non ha valore la presenza di un'autorità centrale che verifichi e controlli le transazioni in quanto, grazie al fatto di essere distribuito, tutti gli utenti posseggono una copia del Ledger che possono visionare e modificare, nel rispetto delle regole che governano il network.

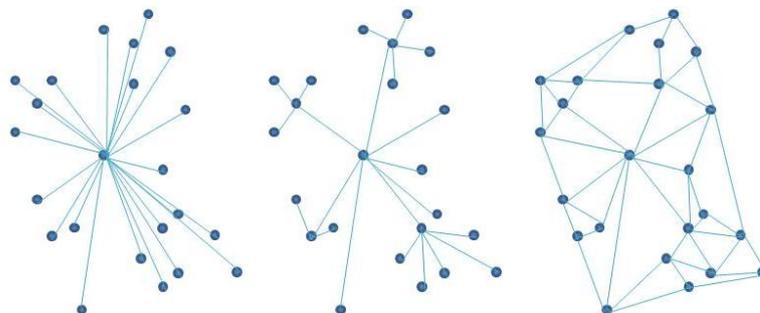


Figura 1 Rappresentazione grafica della differenza tra database centralizzato, decentralizzato e distribuito

Il nome stesso della blockchain suggerisce la filosofia alla base della sua implementazione. Le informazioni vengono immagazzinate in *blocchi* (block) collegati tra loro a creare una *catena* (chain), per cui al crescere del numero delle transazioni, aumenta anche il volume della blockchain. Ogni blocco associa alle transazioni valide una Marca Temporale (*timestamp*) e contiene il proprio *hash*¹ e quello del blocco precedente. Questo impedisce che i blocchi vengano alterati o che ne venga inserito uno tra due già collegati tra loro. Infatti, la blockchain è composta da una serie di client che si aggiornano automaticamente ad ogni operazione effettuata, dopo che questa viene approvata da tutti i singoli nodi attraverso un sistema crittografico che verifica i dati relativi alla transazione (Figura 2).

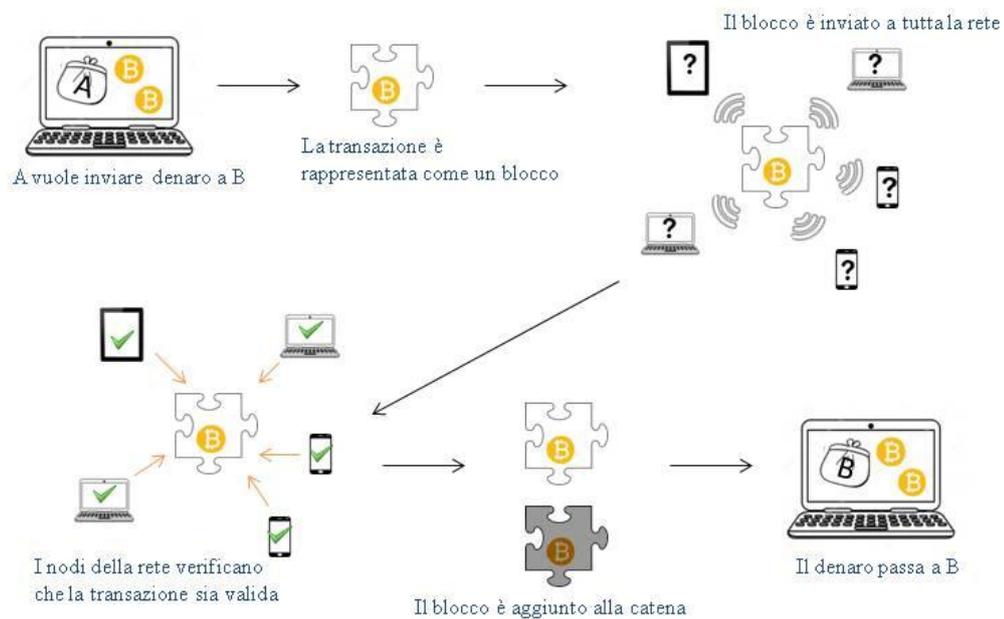


Figura 2 Schema di una transazione sulla blockchain

1.1 Transazioni

Una transazione è il trasferimento di una somma di denaro da un indirizzo A a un indirizzo B. Si possono individuare due tipi di transazioni: quelle P2PKH e quelle Coinbase. Le prime, il cui acronimo significa Pay-to-PubKey-Hash, permettono il trasferimento tra due indirizzi, mentre con le seconde vengono introdotti nuovi Bitcoin nel sistema.

¹ Nel paragrafo 1.4 viene descritto sinteticamente il meccanismo di Hash.

Per capire meglio come avviene una transazione P2PKH attraverso l'utilizzo della blockchain, si può osservare il seguente esempio. Due soggetti intendono effettuare la compravendita di un immobile; vengono create le informazioni relative alla transazione a cui sono applicate le Chiavi Crittografiche specifiche per il venditore e il compratore, come per esempio i dati riguardanti l'immobile, il prezzo, la disponibilità economica dell'acquirente e il certificato di proprietà dell'immobile da parte del venditore. A questo punto la transazione viene immessa nella rete in attesa di essere verificata da tutti i partecipanti alla blockchain; una volta ottenuta l'approvazione, viene creato un nuovo blocco con tutti i dati relativi alla transazione che verrà aggiunto alla catena di blocchi già esistente e sarà accessibile a tutti i partecipanti.

1.2 Mining

Affinché un nuovo blocco contenente più transazioni sia aggiunto alla catena, è necessario che venga controllato, validato e crittografato; solo così può diventare parte della blockchain. Questo passaggio definito *mining* (svolto dai miners) è possibile solo attraverso la risoluzione di un complesso problema matematico che richiede una notevole disponibilità di potenza e di capacità elaborativa.

Qualunque nodo appartenente alla rete può diventare miner e competere per risultare primo nella risoluzione del problema matematico legato alla creazione di un nuovo block valido e, poiché comporta un dispendio di energie, si rende necessaria una adeguata remunerazione dei miners. Nel processo di creazione di nuovi blocchi, ogni miner esegue una serie di passaggi:

- raccolta e decisione di quali informazioni includere nel nuovo blocco tra quelle raccolte dalla rete peer-to-peer;
- verifica della validità delle transazioni incluse;
- selezione del blocco più recente nel ramo più lungo della catena di blocchi e inserimento dell'hash di tale blocco nel nuovo che sta creando;
- tentativo di risoluzione del Proof of Work² per il nuovo blocco e osservazione in contemporanea di quali nuovi blocchi vengono creati da altri nodi:
 - se trova una soluzione al problema del Proof of Work, il nuovo blocco è aggiunto alla catena e condiviso all'interno della rete;
 - se un altro nodo risolve prima il problema, il blocco viene sottoposto a controlli di validità. In caso di successo, questo blocco

² Il meccanismo del Proof of Work viene descritto nel paragrafo 2.1.

viene aggiunto a una copia locale della blockchain; altrimenti, è scartato.

Spesso accade che in un determinato momento siano presenti differenti versioni di blockchain nella rete, dal momento che i miner cercano di creare nuovi blocchi simultaneamente, impiegando la maggior parte del loro tempo a risolvere il problema di Proof of Work. Infatti, vengono creati nuovi blocchi ad un ritmo di 10 minuti circa e in questo lasso di tempo tutti i miner attivi cercano di risolvere il problema. Quando un miner aggiunge un blocco alla catena, viene remunerato con la somma delle commissioni per ogni transazione contenuta nel blocco stesso, oppure attraverso nuove valute come, nel caso più noto, la Blockchain Bitcoin.

Una blockchain può essere Privata (o Permissioned) oppure Pubblica (o Permissionless). In una rete privata, ogni componente ha un'identità unica, che garantisce l'utilizzo delle politiche per limitare la partecipazione alla rete e l'accesso ai dettagli delle transazioni. Con la possibilità di limitazione di accesso, le organizzazioni riescono a rispettare le normative sulla protezione dei dati. Inoltre, poiché una transazione implica diverse e numerose informazioni, i partecipanti coinvolti dispongono della facoltà di specificare quali di queste informazioni possono essere visibili agli altri oppure no. Per esempio, se la Parte A trasferisce un asset alla Parte B, entrambi A e B possono vedere i dettagli della transazione. La parte C vede che A e B hanno interagito, ma non può vedere i particolari relativi all'asset trasferito. La tecnologia che rende possibile questa riservatezza è la *crittografia*³, in particolare l'utilizzo di certificati digitali che come dei passaporti forniscono informazioni identificative, sono resistenti alla contraffazione e possono essere verificati in quanto rilasciati da un ente garantito. Le Blockchain Permissioned quindi richiedono autorizzazioni particolari, stabilite dalle regole di governance vigenti all'interno della rete tra gli operatori predisposti alla gestione degli accessi, ai controlli e all'aggiunta di nuovi blocchi; si uniscono, così, trasparenza, sicurezza e immutabilità alle caratteristiche della blockchain Privata, che la rendono adatta all'impiego in Banche e Pubblica Amministrazione.

1.3 Utenti

All'interno di una rete Blockchain si possono individuare diversi partecipanti con ruoli differenti tra loro:

- utente della blockchain. E' un partecipante con il permesso di unirsi alla rete e concludere transazioni con altri utenti. La tecnologia blockchain

³ Argomento affrontato nel paragrafo 1.4.

opera in background, per cui l'utente non ne ha consapevolezza, né conoscenza;

- regolatore. E' un utente dotato di permessi speciali che gli permettono di avere controllo sulle transazioni che avvengono all'interno della rete. A seconda della governance vigente, ai regolatori potrebbe essere impedito di concludere transazioni;
- sviluppatore. E' il programmatore che crea applicazioni e smart contract che permettono all'utente di utilizzare le funzionalità della rete;
- operatore di rete. E' un individuo dotato di particolari permessi e autorità per definire, creare e gestire la rete;
- piattaforma di elaborazione. E' un sistema di computer utilizzato per aumentare i processi di elaborazione e avviare le richieste nella blockchain;
- fonte dei dati. E' un sistema di dati che fornisce informazioni per definire come avvengono comunicazioni e trasferimenti di dati tra le varie applicazioni;
- autorità di certificazione. E' un individuo che rilascia i certificati necessari al completamento delle transazioni.

1.4 Elementi distintivi della blockchain

Sicurezza e crittografia

Tra le caratteristiche più importanti della blockchain compare senza dubbio la *sicurezza*. Ciò è possibile grazie al concetto di rete Privata o Permissioned come già accennato, ma soprattutto per mezzo di tecniche e processi che assicurano la veridicità delle informazioni scambiate e la loro immutabilità. Infatti, l'impiego di un timestamp e più in generale della crittografia, permette di mantenere la sicurezza su tutta la rete e in qualunque momento.

Innanzitutto, poiché il sistema non prevede un ente centrale di controllo, ogni singola transazione viene resa valida da tutti i nodi per mezzo della Marca Temporale, la quale impedisce che l'operazione venga alterata o annullata: si tratta di "associare data e ora certe e legalmente valide ad un documento informatico, consentendo quindi di associare una validazione temporale opponibile a terzi." (cfr. Art. 20, comma 3 DLgs 82/2005 - Codice dell'Amministrazione Digitale). Il timestamp consiste in una sequenza di caratteri che identificano in modo univoco una data, eventualmente associata a un orario, e si presenta in un formato facilmente comparabile, in modo da poter definire un ordine cronologico degli eventi.

In secondo luogo, la sicurezza è garantita dall'utilizzo di una funzione di tipo crittografico, chiamata Hash. Questa consiste in un algoritmo matematico (per Bitcoin per esempio è SHA 256) che converte in modo univoco dati di lunghezza arbitraria in una stringa binaria di dimensione fissa e presenta la caratteristica di essere unidirezionale, ovvero difficile da invertire. Proprio per il fatto di essere immediato il passaggio da messaggio a codice in hash, ma estremamente complicato il contrario, questo tipo di funzione è estremamente utilizzata - tra le altre - per forme di autenticazione. In una rete blockchain, ogni blocco è identificato da una funzione di hash e inoltre contiene il codice del blocco precedente, in modo che sia impossibile alterarne la sequenza. Proprio l'immutabilità è un altro aspetto molto importante che caratterizza la blockchain: non è possibile apporre modifiche o variazioni; gli eventuali errori possono essere corretti tramite nuove transazioni.

La vera rivoluzione di blockchain (e monete digitali) sta nella modalità di impiego della crittografia. Analizzandola, questa può essere descritta come la scienza che si occupa di proteggere le informazioni rendendole incomprensibili a chiunque non sia il destinatario. Il messaggio da proteggere viene detto testo in chiaro, mentre quello trasformato e reso incomprensibile è chiamato testo cifrato. Il passaggio da testo in chiaro a testo cifrato è detto cifratura; il suo contrario è detto decifratura. La trasformazione, in entrambi i versi, avviene tramite un algoritmo di cifratura (o decifratura), ovvero una procedura che però necessita la conoscenza della cosiddetta chiave crittografica. Solitamente si ipotizza che l'algoritmo di cifratura sia noto a tutti, mentre la chiave sia di conoscenza solamente degli attori coinvolti nella transazione.

Nell'ambito della blockchain, il tipo di crittografia utilizzata è quella asimmetrica o a chiave pubblica (Figura 3). Ognuno possiede due chiavi, una pubblica da distribuire a tutti coloro con cui intende comunicare e una privata da tenere segreta. Nel momento in cui un'informazione viene cifrata attraverso la chiave pubblica (operazione lecita a chiunque, poiché nota a tutti), questa può essere decifrata soltanto attraverso la chiave privata corrispondente (che appartiene al proprietario di quella chiave).

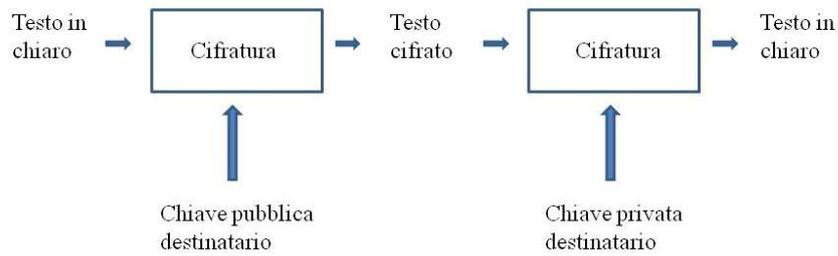


Figura 3 Crittografia asimmetrica

Una novità introdotta dalla crittografia asimmetrica è la firma digitale: il mittente di un messaggio può firmarlo grazie alla sua chiave privata e tutti sono in grado di verificarne l'autenticità tramite la chiave pubblica associata. Attraverso un esempio, si può comprendere meglio il meccanismo (Figura 4). Si ipotizzi che A voglia mandare un messaggio a B: A ricava il digest dell'intero messaggio tramite la funzione di hash, lo cifra attraverso la propria chiave privata e allega il digest cifrato, che costituisce una sorta di firma, al messaggio completo; questo viene interamente cifrato per mezzo della chiave pubblica di B. Successivamente, il destinatario del messaggio utilizza la propria chiave privata per decifrare il messaggio; ne calcola il digest e lo confronta con quello che ottiene decifrando con la chiave pubblica del mittente la firma allegata: se coincidono la firma è autentica.

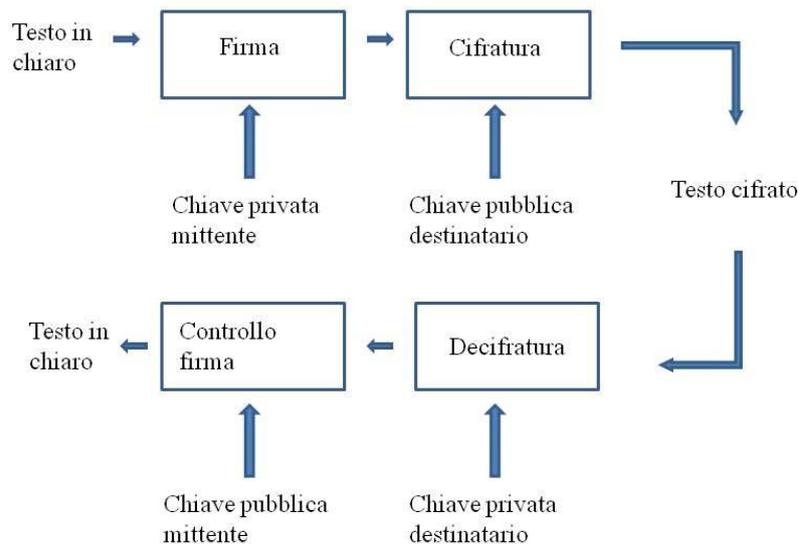


Figura 4 Crittografia e firma digitale

Fiducia o Trust

Il secondo concetto alla base della blockchain è la *fiducia*: per permettere il funzionamento in un ambito commerciale è necessario che sussista fiducia tra le parti che effettuano una transazione. Per come viene strutturata la rete, in realtà, tale nozione di fiducia è oltrepassata, non è indispensabile. Infatti, è la rete stessa a decretare fiducia tra i partecipanti perché ogni transazione si appoggia alle precedenti, ogni alterazione è subito visibile a tutti e risulta quasi immediato verificare la conformità delle operazioni.

Altre caratteristiche

Le altre caratteristiche che rendono di grande interesse questa tecnologia sono:

- affidabilità: non esistendo un centro da cui parte il controllo, tutti i partecipanti vigilano sull'intera rete e anche in caso di attacco a un nodo che ne risulta danneggiato, tutti gli altri nodi continuano a essere operativi;
- trasparenza: le operazioni che avvengono nella rete sono visibili a tutti i partecipanti;
- convenienza: nelle transazioni tradizionali è necessaria una terza parte come interlocutore, mentre nella blockchain viene meno questa esigenza;
- solidità: le informazioni presenti nella rete non possono essere alterate, ma rimangono sempre attendibili e immutate;
- irrevocabilità: una volta effettuata una transazione, questa non può essere annullata;
- digitalità: tutto diventa virtuale, permettendo l'applicazione della blockchain in numerosi ambiti.

1.5 Token

Per la necessità di scambiare un asset digitale tra due parti senza l'azione di un intermediario, sono stati introdotti i cosiddetti token. Un token è un "pacchetto" di informazioni digitali registrate su una blockchain che permette di conferire un diritto di proprietà a un soggetto sulle informazioni contenute nel token stesso. Nel caso in cui il token incorpori diritti addizionali, il sistema è regolato dagli smart contracts. Il primo esempio di token è stato il Bitcoin, ma in seguito ne sono nati diversi e con caratteristiche differenti.

A tal proposito è utile distinguere i tipi di token disponibili, che si distinguono tra loro per approccio tecnologico e per utilizzo. In particolare, si possono menzionare:

- token di classe 1: si presenta come una vera e propria moneta, viene trasferito per mezzo di transazioni su blockchain e non prevede nessuna controparte, in quanto non conferisce diritti nei confronti di quest'ultima, ma semplicemente registra un diritto di proprietà del token stesso. In questa categoria rientrano le criptomonete.
- token di classe 2: permette di conferire al proprietario dei diritti verso delle controparti, ovvero che possono essere esercitati nei confronti del soggetto che ha generato il token stesso. Si potrebbe parlare quindi di una forma di titoli di credito, nel senso di documenti che conferiscono al possessore “*diritto alla prestazione in esso indicata verso presentazione del titolo*” (art. 1992 c.c.), ovvero titoli obbligazionari, di partecipazione, di prestito, di legittimazione e rappresentativi di merci.
- token di classe 3: con funzione mista, permette di rappresentare diritti di comproprietà ma al tempo stesso conferisce diritti diversi (di voto, di tipo economico..).

Esiste un'altra forma di classificazione dei token, proposta dall'ente svizzero FINMA ⁴, che distingue tre tipologie a seconda delle caratteristiche:

- Payment token: sono le criptovalute accettate spesso anche come forma di pagamento e per questo definiti più spesso come coin che come token.
- Utility token: asset che permettono l'accesso a servizi digitali o applicazioni.
- Security o Asset token: valori patrimoniali digitali soggetti alle norme degli enti regolatori finanziari. In termini di funzione economica, i token sono analoghi ad azioni, obbligazioni o derivati.

1.6 Ambiti di utilizzo

Dal punto di vista dell'applicazione nelle attività commerciali, la blockchain presenta innumerevoli vantaggi. Innanzitutto permette un risparmio in termini di tempo, perché le transazioni non necessitano dell'approvazione di un ente centrale e anche quelle più complesse richiedono pochi minuti. Un secondo tipo di risparmio è quello dei costi, in quanto le spese sono notevolmente ridotte: non è richiesta la supervisione di una terza parte, gli intermediari praticamente spariscono perché gli scambi avvengono in maniera diretta tra le parti e non c'è duplicazione dello sforzo in quanto tutto è visibile in un registro condiviso. Infine, come già detto, garantisce la sicurezza delle transazioni.

⁴ Il 16 febbraio 2018, l'Autorità di vigilanza sui mercati finanziari (FINMA - Swiss Financial Market Supervisory Authority) ha pubblicato una guida pratica che spiega come tratta le domande inerenti all'assoggettamento in riferimento alle initial coin offering.

Smart Contract e Ethereum

Come indicato, la blockchain è un tecnologia, un paradigma che sta alla base di numerose applicazioni reali. Le più rappresentative sono le *criptomonete* e gli *smart contracts*; per le prime si rimanda al prossimo capitolo.

Uno Smart Contract (o self-executing contract o contratto digitale) è un accordo o insieme di direttive che regolano un'operazione commerciale; questo viene registrato nella rete e viene eseguito in modo automatico come parte della transazione (Figura 5). La sua particolarità risiede nel fatto di richiedere un supporto legale per la sua stesura, ma non per la sua verifica, né per la sua attivazione. Infatti, uno Smart Contract è la trascrizione in codice di un contratto, in modo che sia possibile verificare in maniera automatica l'avverarsi di determinate condizioni concordate dalle parti e che vengano, di conseguenza, eseguite in automatico azioni. Per l'assenza di un'intromissione umana e quindi di un contributo di tipo interpretativo, lo Smart Contract deve presentare esposizioni estremamente dettagliate di tutte le contingenze, situazioni e condizioni che devono essere considerate, oltre a una serie di regole precise da rispettare per permettere al contratto di essere eseguito. Una volta elaborato il contratto, è il programma a eseguirlo come un codice, per cui da un punto di vista legale si ha la certezza dell'oggettività del giudizio che esclude ogni possibile forma di interpretazione; al tempo stesso assume un ruolo rilevante la programmazione e lo sviluppo del codice, in quanto rappresenta un momento di responsabilità decisionale.

Ethereum è forse il caso più famoso di utilizzo della rete blockchain per gli Smart Contracts. Parallelamente a Blockchain e Bitcoin, negli ultimi anni si è sviluppato un filone di progetti che si volevano distaccare dall'immagine di protocolli alla base di nuove monete virtuali. Il focus, infatti, è puntato sullo sviluppo di DLT di tipo Open Source, che permettono diverse opportunità di utilizzo. In questo contesto ha avuto origine Ethereum: progetto nato con le caratteristiche di blockchain pubblica nella forma di piattaforma di *distributed computing open source*, ideata per mettere a disposizione la possibilità di creare e gestire, come detto, Smart Contract in modalità peer-to-peer.

"Lo scopo di Ethereum è quello di creare un protocollo alternativo per la costruzione di applicazioni decentralizzate, fornendo un insieme eterogeneo di possibilità che, [...], saranno molto utili per una larga classe di applicazioni decentralizzate, in particolar modo nelle situazioni dove sono essenziali: un tempo rapido di sviluppo, la sicurezza per applicazioni utilizzate di rado, e la capacità di far interagire tra loro, in modo molto efficace, applicazioni differenti. Ethereum permette tutto ciò attraverso la costruzione di quello che in sostanza è il definitivo protocollo astratto e fondante: una Blockchain con un linguaggio di

programmazione, [...], che permette ad ognuno di scrivere Smart Contracts ed applicazioni decentralizzate dove stabilire le proprie regole arbitrarie per la proprietà, i formati delle transazioni e le funzioni di transizione di stato."⁵

Si può quindi definire Ethereum come una piattaforma per computing distribuito che si appoggia alla cosiddetta Ethereum Virtual Machine (EVM), ovvero un computer che non esiste fisicamente ma solo sulla Rete, distribuito, condiviso e immutabile. Al suo interno tutte le transazioni sono regolate e remunerate attraverso una criptomoneta calcolata in Ether.

La differenza sostanziale con la Blockchain e i Bitcoin e ciò che rende Ethereum davvero interessante dal punto di vista tecnologico, è che non offre soltanto la possibilità di operazioni predefinite e standardizzate, ma permette agli utenti di creare le proprie *operations*, non necessariamente limitate alle criptovalute. Queste operation generalmente sono contenute all'interno degli Smart Contract, che "possono essere sbloccati solo se si verificano certe condizioni, inoltre possono essere anche costruiti sull'apice della piattaforma, con degli strumenti molto più efficaci di quelli offerti dallo scripting del Bitcoin, grazie agli strumenti offerti dalla completezza del linguaggio di Turing, consapevolezza del valore, dello stato e della blockchain."⁶

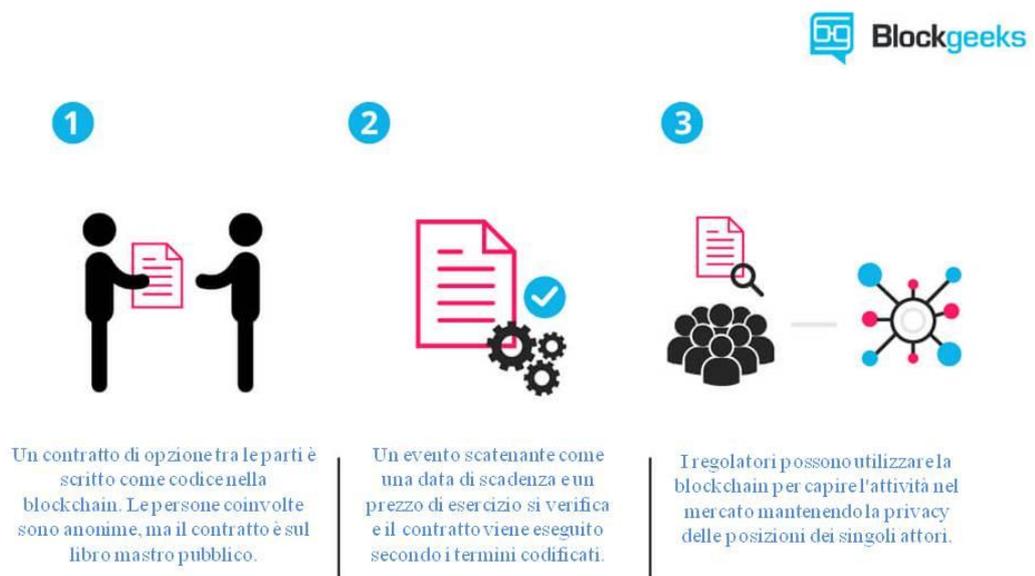


Figura 5 Schema di uno Smart Contract, Blockgeeks

⁵ Da "Ethereum: Libro Bianco - White Paper", Leonardo Maria Pedretti, pag. 8

⁶ Da "Ethereum: Libro Bianco - White Paper", Leonardo Maria Pedretti, pag. 8

Altri ambiti

Un modo per capire ulteriormente la tecnologia blockchain e apprezzare la sua potenzialità è considerare anche gli altri suoi casi d'uso, tenendo a mente che essendo un paradigma in evoluzione, la lista delle sue applicazioni è in continua espansione.

Servizi finanziari. Finanza ed economia sono i due settori per eccellenza coinvolti dalla blockchain, che si presenta come lo strumento per abbattere costi di commissione delle banche e per garantire velocità, affidabilità e sicurezza delle transazioni.

Assicurazioni. La possibilità di transazioni sicure e decentralizzate, attuate in modo che non siano possibili frodi e manipolazioni, rappresenta un incentivo per le assicurazioni; inoltre è possibile avere notifiche aggiornate e accurate a proposito dei cambiamenti e ciò permette una migliore gestione del rischio, senza contare che si possono ottenere informazioni sicure sui propri clienti.

Pubblica Amministrazione e Sanità. Moltissime operazioni governative implicano transazioni e registrazioni di proprietà di asset; con la rete blockchain è facile assicurare trasparenza ed efficienza. Al tempo stesso, il Governo potrebbe avere costantemente aggiornate le informazioni sull'identità della popolazione attraverso l'utilizzo di un ID digitale con lo scopo, per esempio, di rendere più difficile l'evasione fiscale o di avere un controllo maggiore dei cittadini per combattere la criminalità.

Per quanto riguarda l'ambito della sanità, la possibilità di gestire dati medici dei pazienti attraverso un sistema condiviso, garantirebbe ai medici la condivisione di informazioni sui pazienti in maniera sicura e veloce, per arrivare a una cura più precisa e in tempi più rapidi.

Supply chain. La blockchain registra la provenienza e i dettagli relativi a ogni componente o materia prima implicati in un processo produttivo. In ambito agroalimentare aumenta l'affidabilità del produttore e del prodotto nonché la sua tracciabilità.

Nota sulla nomenclatura

Se finora si è usato genericamente il termine blockchain, è da sottolineare che esiste una precisa distinzione tra il nome scritto con iniziale minuscola e quello scritto con iniziale maiuscola: il primo sta ad indicare la tecnologia in sé, un network che può essere implementato e utilizzato da chiunque e di cui ne esistono molteplici versioni differenti; nel secondo caso, invece, si fa riferimento a una delle implementazioni della tecnologia, in particolare alla più famosa che è legata ai Bitcoin.

CAPITOLO 2

2. Criptovalute e Bitcoin

Una criptovaluta è una valuta digitale e decentralizzata ideata per operare come mezzo di scambio e che utilizza la crittografia per rendere sicure le transazioni, controllare la creazione di nuove unità e verificare il trasferimento di asset.

Al fine di evitare la contraffazione, viene spesso utilizzato come sistema di implementazione uno schema *Proof of Work*. Le criptomonete sfruttano tecnologie peer-to-peer su reti in cui i nodi sono i computer di utenti che, per partecipare agli scambi, eseguono particolari programmi che fungono da portamonete. A differenza dei sistemi tradizionali di pagamento, non esiste una gestione di tipo centralizzato e il rilascio di nuove unità di moneta avviene in rete in modo collettivo.

La creazione e l'utilizzo di una criptovaluta porta vantaggi tra i quali, come già detto, l'impossibilità di falsificazione, l'abbattimento dei costi e dei tempi di transazione rispetto ai circuiti tradizionali e l'indipendenza del suo valore dalle crisi economiche e monetarie, essendo svincolata da qualunque sistema bancario o governativo.

Al tempo stesso, però, le criptomonete presentano criticità come la notevole difficoltà di conversione degli importi nei corrispondenti valori espressi in valute tradizionali; spicca soprattutto l'elevato costo in caso di produzione (o Mining) in termini di energia e potenza di calcolo.

2.1 Mining

Focalizzando l'attenzione sul *mining*, ovvero la fase di creazione delle criptovalute, è necessario premettere che queste ultime sono state ideate in modo tale che nuove unità di valuta siano introdotte gradatamente fino a raggiungere un tetto massimo prestabilito della quantità di moneta in circolazione; le ragioni sono principalmente due: evitare una crescita esponenziale dell'inflazione e imitare la scarsità, e il conseguente valore, dei metalli preziosi. Quando fu progettata la rete Blockchain, infatti, emerse il problema di come emettere nuova moneta: facendo riferimento alle valute tradizionali, i sistemi monetari mondiali emettono moneta attraverso le banche centrali che ne stabiliscono il valore in base al mercato e all'oro. Ma in una rete decentralizzata come la Blockchain, anche il sistema di emissione deve essere coerente con questa impostazione. La soluzione quindi è rappresentata dal mining, ovvero il sistema utilizzato per emettere la valuta in

questione. Come già visto nel capitolo precedente, al fine di aggiungere un nuovo blocco contenente transazioni alla catena, è necessario che venga risolto un complesso algoritmo matematico da un cosiddetto miner; questo è ricompensato con una certa quantità di criptomoneta, a cui si somma una percentuale su tutte le transazioni inserite nel blocco.

Da un punto di vista tecnico, il mining di una criptovaluta consiste in un'operazione di *brute forcing* - ovvero un algoritmo di risoluzione in cui vengono verificate tutte le soluzioni possibili dal punto di vista teorico fino a trovare quella corretta - che ha come scopo quello di trovare un numero che rispecchi determinate caratteristiche (o target) legate ai concetti di crittografia, da inserire in un insieme di dati; la sua difficoltà varia in modo dinamico a seconda del target posto come obiettivo. Questa operazione fa parte del cosiddetto *Proof of Work* (Figure 6, 7, 8). I miner competono tra di loro per risolvere l'algoritmo; per dimostrare di essere arrivato prima degli altri alla soluzione corretta, il miner deve dare una prova dello svolgimento del suo lavoro, ovvero fornire il numero trovato. Si tratta di un sistema costoso in termini di potenza richiesta, in quanto la probabilità di vincere e ricevere la ricompensa dipende dal rapporto tra la potenza hardware locale e quella complessiva.

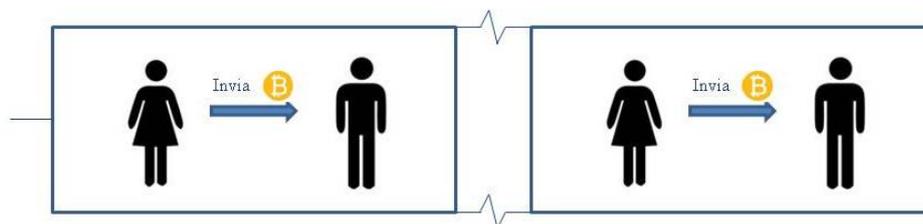


Figura 6 Rappresentazione della PoW, parte 1

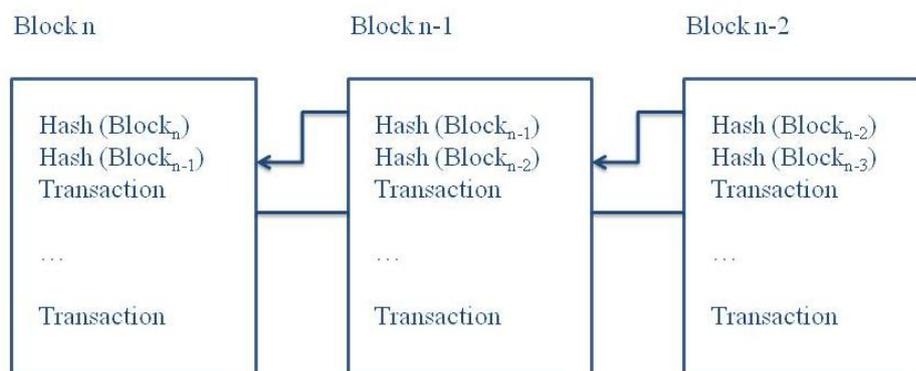


Figura 7 Rappresentazione della PoW, parte 2

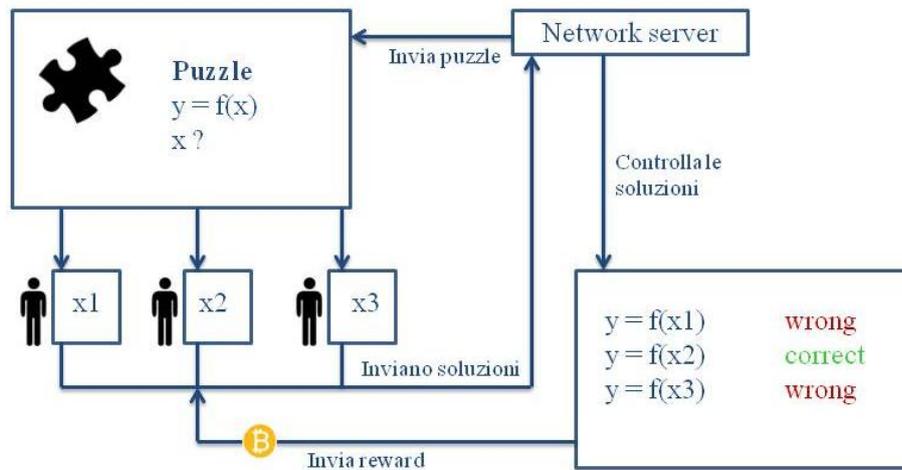


Figura 8 Rappresentazione della PoW, parte 3

Quindi, la complessità del problema dipende dal numero di utenti presenti nella rete, dalla potenza di calcolo disponibile e dal carico della rete. La hash (termine con cui si indica sia il problema matematico, sia la sua soluzione) di ogni blocco contiene la hash del blocco precedente, in modo da incrementare la sicurezza e da impedire ogni possibile violazione informatica.

I motivi per cui si è imposto il modello basato sulla Proof of Work sono principalmente due. In primo luogo, protegge la rete da possibili attacchi DoS, in quanto un attacco efficiente richiederebbe grandi quantità di tempo e potenza di calcolo; secondariamente, non ha importanza la quota posseduta nel proprio portafoglio, perciò a ingenti somme di denaro non corrisponde necessariamente un maggiore controllo della rete, dal momento che si tiene in considerazione solamente la capacità di calcolo.

Al crescere della popolarità e dell'utilizzo delle criptomonete, e di conseguenza del mining, è corrisposto un aumento della potenza elaborativa della rete. L'effetto scaturito è stato un aumento della difficoltà e quindi una diminuzione del possibile guadagno giornaliero per singola macchina; questo ha fatto sì che alcuni miner si unissero nelle cosiddette *mining pool*, ovvero gruppi con lo scopo di ottenere un afflusso di moneta più consistente e costante rispetto al mining in solitaria. Pian piano si è quindi creata una domanda e un mercato, ma soprattutto le criptomonete hanno ottenuto un valore tangibile e una certa liquidità.

Come naturale conseguenza, è nato il mining professionale, ovvero la costruzione di potenti macchine ad hoc costantemente accese per fare mining e rivenderne il ricavato sul mercato. Un effetto secondario di questo fenomeno è l'aumento dei prezzi dovuto alla *corsa all'hardware*, di cui risente anche un qualunque utente

che vuole acquistare un computer nuovo. Ma il fatto degno di nota che desta più preoccupazione è sicuramente l'ingente consumo di energia elettrica impiegata per l'attività di mining: l'analista di criptovalute Alex de Vries, conosciuto come Digiconomist⁷, stima che ai prezzi attuali, i miner di Bitcoin impieghino oltre 24 terawattora di elettricità all'anno mentre competono per risolvere i puzzle crittografici sempre più difficili, ovvero tanto quanto la Nigeria, un Paese di 186 milioni di persone, utilizza in un anno. Certamente non un'attività eco-friendly e sostenibile.

Per ovviare a questo problema, alcune criptovalute hanno iniziato a implementare un algoritmo alternativo, ovvero il Proof of Stake; la differenza principale è che la quantità di CPU/GPU richiesta è minore.

2.2 Double Spending

Il digitale è per sua natura duplicabile all'infinito, basti pensare alla capacità di rendere disponibile un bene o un servizio in modo illimitato (come per esempio un software, un ebook o una canzone) a qualunque cliente lo richieda, sempre nella stessa forma e a costi decisamente più bassi rispetto a quelli che caratterizzano il mondo materiale. Questa opportunità però non garantisce che un determinato bene o servizio sia duplicato sempre nel rispetto delle regole di business o etiche: succede quindi che anche le monete digitali subiscano una duplicazione non legale. Se si crea la copia esatta di una moneta, e quindi si ha la possibilità di pagare due o più volte per beni differenti, si manifesta un problema di frode che mina le basi di qualsiasi relazione commerciale. Questo fenomeno è indicato come Double Spending e la blockchain offre un meccanismo per impedire che ciò venga messo in atto: il problema di coordinare un gruppo di nodi al cui interno si possono nascondere dei sabotatori è conosciuto come Problema dei Generali Bizantini (Byzantine fault tolerance - BFT). La blockchain risolve il problema sfruttando la potenza computazionale dei nodi come sistema di voto; attraverso la verifica del valore di hash si stabilisce l'ordine cronologico dei blocchi inseriti nella catena e, in caso di duplicazioni, si dà precedenza al primo che è stato creato.

⁷ https://motherboard.vice.com/en_us/article/ywbbpm/bitcoin-mining-electricity-consumption-ethereum-energy-climate-change

2.3 Bitcoin

Attualmente l'applicazione più utilizzata della Blockchain - e ciò che l'ha resa così famosa - è il sistema dei Bitcoin (BTC).

Installando sul proprio dispositivo una delle applicazioni disponibili per il portafoglio Bitcoin, è possibile accedere al servizio che permette di utilizzare la valuta Bitcoin come moneta di scambio. Osservando il protocollo alla base del sistema, una transazione può essere interpretata come la volontà di un utente di diminuire la propria quota di Bitcoin per aumentare dello stesso valore la quota di un secondo utente. Innanzitutto viene generato un primo indirizzo Bitcoin, condivisibile con chiunque, che permette di inviare denaro a tale indirizzo. Tutte le transazioni validate sono salvate da ogni nodo della rete e attraverso il proprio portafoglio virtuale si può conoscere quanti Bitcoin rimangono a disposizione per effettuare altre operazioni. Come visto precedentemente, il denaro viene trasferito tra due portafogli Bitcoin e questa operazione viene resa sicura attraverso una chiave privata al fine di garantire che il denaro trasferito sia effettivamente della persona che ha eseguito la transazione e assicurare così protezione dell'operazione stessa.

Un portafoglio (o *wallet*) digitale contiene uno o più indirizzi bitcoin, ognuno dei quali associato a un numero variabile di bitcoin. Ogni indirizzo, che rappresenta la chiave pubblica, è associato a una firma digitale, ovvero la chiave privata, per garantire che solo il proprietario di un certo indirizzo possa iniziare un'operazione legata ad esso, come già visto nel paragrafo 1.4. Proprio per mezzo della chiave pubblica si garantisce sicurezza alle transazioni, o in alternativa sfruttando il controllo degli input pregressi che permette di controllare che il mittente posseda veramente la cifra in Bitcoin necessaria alla transazione.

Di ogni transazione viene memorizzato il codice identificativo del mittente, quello del ricevente e la quantità di bitcoin trasferiti; i due codici sono anonimi, ovvero non permettono di risalire all'identità delle parti che eseguono l'operazione.

Alcuni siti permettono di vedere in tempo reale il susseguirsi di transazioni, come per esempio <https://blockchain.info> da cui è presa la seguente schermata⁸ (Figura 9). Cliccando su una qualunque delle righe è possibile conoscere maggiori dettagli riguardo alla specifica operazione.

Altra caratteristica dei Bitcoin è quella di tendere in modo asintotico al limite dei 21 milioni di unità. La disponibilità di nuove monete cresce ogni 4 anni seguendo una serie geometrica; raggiunta la data in cui saranno disponibili tutte le monete e ipotizzando che la richiesta di Bitcoin aumenti nel tempo, questi subiranno un aumento del loro valore reale (deflazione) a causa della loro scarsità.

⁸ Aggiornata alla data 6/11/2018.

[<< Precedente](#) **Blocchi prodotti su:06/11/2018** [Successivo >>](#)

Altezza	Orario	Inoltrato da	hash	Dimensione (kB)
549046 (Catena Principale)	2018-11-06 20:49:48	AntPool	0000000000000000000000007e284e8093cb006e77ca4412d8c2949903bf116b31032	1,203.19
549045 (Catena Principale)	2018-11-06 20:47:51	Unknown	000000000000000000000000114bb162879f41e18524d43e3c0b1390d1b6ae46c502b4	1,406.45
549044 (Catena Principale)	2018-11-06 20:38:22	ViaBTC	000000000000000000000000f4af1e482a2fe1f1e23f0b376d2e0c6c53def4046c90	1,241.14
549043 (Catena Principale)	2018-11-06 20:11:47	BitFury	00000000000000000000000074cb620fc405c143a6d5b19cadce154aabb1c3ddb919	1,301.26
549042 (Catena Principale)	2018-11-06 19:52:41	Unknown	000000000000000000000000101e4c42f083edf8e617d7bb1b970339b71ebe59c9016	1,242.6
549041 (Catena Principale)	2018-11-06 19:38:59	AntPool	000000000000000000000000dc731749c7a62c7fdcdacfd168dd04341c0fc96c21cf	1,161.84
549040 (Catena Principale)	2018-11-06 19:25:32	F2Pool	00000000000000000000000063c905023e0d7fb76fd271bc9440807a69d812d35e7a	1,217.51
549039 (Catena Principale)	2018-11-06 19:22:07	F2Pool	000000000000000000000000c71775a7f376597617dce2618394a9c20fde264849aa	1,270.93
549038 (Catena Principale)	2018-11-06 19:20:00	Unknown	000000000000000000000000206fc3ddb64fba6fb2b0217285ff1a59e8add0b0da82f1	1,175.46
549037 (Catena Principale)	2018-11-06 19:15:10	BTC.com	000000000000000000000000a7a936668b4ade3638ee0a87312760f6903ad4db53ff2	1,328.74
549036 (Catena Principale)	2018-11-06 18:49:47	BTC.com	0000000000000000000000006918cfa9c68365b6ea8c8c266d6b77c478b7375464b8c	1,189.09
549035 (Catena Principale)	2018-11-06 18:33:27	Unknown	000000000000000000000000161cf0d0bc50e082d5cce4bb7348bdc83455660879d671	1,224.72

Figura 9 Screenshot da <https://blockchain.info>

Ma i Bitcoin non sono l'unica valuta nata in ambito digitale. Le criptomonete più conosciute sono Ethereum, Bitcoin Cash, Litecoin, NEM, IOTA, Cardano; la lista potrebbe essere molto più lunga considerato che attualmente le criptovalute sono più di un migliaio. Di seguito saranno descritte le principali caratteristiche di alcune delle più importanti dopo i Bitcoin, ordinate per capitalizzazione di mercato⁹.

2.4 Ethereum ETH

Ethereum può essere considerata come la più importante criptomoneta di seconda generazione. Consiste in una blockchain programmabile in cui gli sviluppatori possono realizzare applicazioni decentralizzate, denominate DApps. Analogamente alla Blockchain associata ai Bitcoin, Ethereum presenta come valuta Ether, con la differenza che è implementato un metodo Proof of Stake. L'aspetto innovativo di Ethereum è la possibilità di effettuare gli smart contracts, cioè accordi digitali eseguibili quando si verificano le condizioni stabilite dalle parti.

⁹ Dati presi da <https://coinmarketcap.com/> in data 6/11/2018. Nell'ordine, le prime venti criptomonete sono: Bitcoin, Ethereum, XRP, Bitcoin Cash, EOS, Stellar, Litecoin, Cardano, Monero, Tether, TRON, Dash, IOTA, Binance Coin, NEO, Ethereum Classic, NEM, Tezos, Zcash, VeChain.

2.5 Ripple XRP

Nata nel 2013 con uno spiccato orientamento verso il mondo bancario, rappresenta ad oggi una delle migliori alternative a criptovalute come Ethereum e Bitcoin. Si tratta di una tecnologia che permette alle banche di effettuare in tempo reale scambi di moneta attraverso una rete finanziaria; infatti, Ripple semplifica il pagamento creando dei trasferimenti punto-punto, senza la necessità di pagare commissioni. Ripple è, quindi, un mezzo che le banche possono utilizzare per velocizzare pagamenti a livello globale, rendendoli a basso costo e immediatamente disponibili indipendentemente dalla tipologia e dal quantitativo. Come conseguenza è possibile ottenere nuove opportunità di investimento, una user experience migliorata e costi di processo inferiori. Al momento 15 grandi banche internazionali lavorano con Ripple e sono 9 i Paesi che utilizzano questa criptovaluta.

Il suo funzionamento si differenzia notevolmente rispetto al Bitcoin. Innanzitutto, Ripple è un network per banche in cui sono possibili trasferimenti di denaro in differenti valute, la principale delle quali è appunto Ripple. Inoltre, il network è di tipo centralizzato, motivo per cui potrebbe non essere considerata a tutti gli effetti come una criptomoneta libera, ma una sorta di via di mezzo che sfrutta la tecnologia delle criptovalute per permettere pagamenti di tipo classico.

2.6 Bitcoin Cash BCH

Nata nell'agosto 2017, questa criptovaluta presenta una storia singolare: alcuni programmatori della Bitcoin Community, con l'esigenza di realizzare un sistema più veloce e adeguato al commercio, hanno eseguito un'operazione che in gergo si chiama *hard fork* del software, creando appunto Bitcoin Cash. Chiunque possedesse Bitcoin, in seguito alla suddetta scissione si è ritrovato nel proprio wallet anche l'equivalente in Bitcoin Cash.

I BCH sono usati essenzialmente per operazioni di investimento tramite dei contratti finanziari chiamati CFD che, sotto il controllo di autorità di vigilanza (la CONSOB in Italia, per esempio), permettono di investire sul Bitcoin Cash senza acquistarlo.

2.7 Litecoin LTC

Litecoin è stata una tra le prima valute digitali ad affermarsi dopo Bitcoin; le differenze riguardano il modo in cui opera e gli algoritmi con cui si possono ottenere Litecoin. Già dal nome si intuisce la volontà di essere più "leggera": Litecoin, infatti, genera blocchi ogni 2,5 minuti, ovvero a un tasso circa quattro volte più veloce a quello di Bitcoin, cosa che comporta una notevole riduzione dei tempi d'attesa per la conferma di una transazione. Cambia anche l'algoritmo crittografico, ovvero Scrypt, che permette di fare mining anche su normali computer; nonostante questo, è meno diffuso rispetto all'algoritmo di Bitcoin ritenuto più sicuro. Come i BTC, anche Litecoin ha un tetto massimo di unità che è possibile produrre e che si aggira intorno agli 84 milioni.

Una curiosità: il suo fondatore Charlie Lee ha recentemente venduto tutte le sue quote di LTC al fine di evitare le costanti accuse di insider trading; ogni suo commento pubblico, infatti, aveva la capacità di variare sensibilmente la valutazione della criptomoneta.

2.8 Dash DASH

Questa criptomoneta si propone di sostituire il denaro tradizionale. Le sue transazioni sono istantanee grazie all'utilizzo combinato dei sistemi Proof of Work e Proof of Stake e all'introduzione di un secondo livello del network che include i *Master Node*, ovvero nodi con un'importanza maggiore rispetto agli altri partecipanti alla rete. Dash prevede anche le funzioni *Instant Send* e *Private Send*, con le quali si ottengono rispettivamente transazioni in meno di un secondo e un aumento del livello di privacy sull'operazione.

2.9 Iota IOT

E' la prima criptomoneta senza fee nelle transazioni e infinitamente scalabile, in quanto sfrutta il sistema Tangle, ovvero un Grafico Diretto Aciclico sulla tradizionale blockchain. Iota si prefigge l'obiettivo di fornire comunicazioni e transazioni sicure tra le macchine nello scenario dell'*Internet of Things* (IoT, Internet delle Cose). Questa criptovaluta si basa su una tecnologia che non richiede la figura del miner, in quanto tutte le unità disponibili di Iota sono già state rilasciate al momento della fornitura iniziale. Inoltre, è davvero una moneta decentralizzata perché, al fine di effettuare una transazione, bisogna convalidarne altre due attraverso il software che permette l'accesso al proprio wallet.

2.10 Nem XEM

Il suo nome è l'acronimo di New Economy Movement, ad indicare quanto la blockchain sia portatrice di una rivoluzione economica. NEM è una variante della Blockchain che si basa sul processo della *Proof of Importance* POI, su un meccanismo per il controllo della reputazione noto come *EigenTrust*, su account multi firma e sulla possibilità di messaggistica criptata.

Oltre agli scenari economico-finanziari, NEM ambisce all'impegno sociale in quanto i fondatori danno risalto alla volontà di utilizzare la Blockchain e la sua tecnologia per cercare soluzioni alla questione della disuguaglianza nella distribuzione della ricchezza. L'obiettivo è dunque quello di operare in un ambiente caratterizzato da pari opportunità, dal principio di decentramento e da libertà finanziaria.

CAPITOLO 3

3. Card

Questa tesi si propone di analizzare l'impiego della blockchain nel campo delle gift card e loyalty card. Per procedere con la discussione, però, è necessario chiarire cosa siano le suddette card; con questo capitolo, quindi, se ne spiega sinteticamente il funzionamento.

3.1 Gift Card

Cos'è e come funziona

Una gift card o carta regalo è una carta di pagamento elettronico prepagata che contiene una quantità specifica di denaro disponibile per l'uso su un'ampia varietà di acquisti.

Quello della carta regalo è uno strumento sempre più scelto dai retailer per invogliare i consumatori allo shopping. Al momento dell'acquisto della carta, il consumatore corrisponde alla società emittente l'importo pari al valore della medesima, del quale potrà fruire, lui stesso o il soggetto che ne entrerà in possesso, per l'acquisto, in una o più soluzioni, dei beni o servizi venduti dalla società. Non è inusuale trovare gift card di importi preimpostati, in ogni caso molte di queste hanno un carico iniziale che oscilla all'interno di un range (di solito 10-500€). Come precauzione, per mitigare il rischio di smarrimento, molte carte regalo possono anche essere registrate online; ciò consente di tenere traccia e congelare il saldo rimanente in caso di perdita di una carta.

Generalmente, possono essere individuati due tipi di gift card: carte aperte e chiuse, ed entrambe sono utilizzate sia online sia di persona.

Carte a circuito chiuso

Le carte a circuito chiuso di norma permettono il loro utilizzo solamente presso un singolo venditore; sono spesso commercializzate dai rivenditori che consentono ai clienti di caricare fondi prepagati i quali possono essere impiegati per acquisti futuri e di solito non richiedono alcuna quota di attivazione. Questa tipologia di gift card in genere non è ricaricabile, quindi una volta che il saldo è esaurito, non permette un secondo utilizzo.

Carte a circuito aperto

Le carte a circuito aperto offrono l'equivalente di denaro contante che può essere utilizzato presso qualsiasi esercizio commerciale in cui il processore della carta di pagamento è accettato. Solitamente si tratta di uno dei principali processori, come

Visa, MasterCard o American Express. Queste carte visualizzano il logo del processore di pagamento e possono essere utilizzate per effettuare tutti i tipi di pagamenti elettronici pressoché ovunque.

Le gift card a circuito aperto hanno anche il vantaggio di poter fungere da carta prepagata standard: poiché sono generalmente ricaricabili, permettono all'utente di aggiungere fondi per conto proprio. A volte le carte a circuito aperto richiedono una piccola quota di attivazione addebitata al momento dell'acquisto e dell'attivazione della carta.

Entrando più nello specifico, nell'ordinamento italiano le gift card non hanno una disciplina distinta e unitaria e pertanto, per individuarne la regolamentazione, è necessario fare riferimento alla disciplina delle carte prepagate in generale. La carta regalo si qualifica come carta prepagata “chiusa”: viene accettata solo per il pagamento dei beni offerti dalla società che la emette e non può quindi essere usata come mezzo di pagamento generale, non essendo cioè “moneta elettronica”. L'utilizzo di tale carta deve essere retto da condizioni generali di utilizzo predisposte dalla società che la emette e dovranno essere portate alla conoscenza del consumatore, inoltre non dovranno essere per lui vessatorie.

Vantaggi

Analizzando i vantaggi legati all'utilizzo di carte regalo, è possibile distinguere tra quelli relativi ai clienti e quelli invece per i retailer.

Innanzitutto, il consumatore finale è attirato dalle gift card in quanto semplifica il processo d'acquisto. In occasione di eventi speciali e ricorrenze, risolve il problema di un regalo sbagliato (magari nella taglia) o non gradito, permettendo a chi lo riceve di scegliere direttamente e in prima persona ciò che preferisce.

La carta regalo, inoltre, garantisce praticità e immediatezza poiché rappresenta una sorta di salvadanaio sempre a disposizione. Spesso alle gift card sono legati sconti e promozioni che costituiscono, quindi, un incentivo per il consumatore che vede un vantaggio nell'utilizzo di questo strumento.

Dal punto di vista dei retailer, invece, le carte regalo rappresentano la possibilità di cash flow immediato, con conseguente agevolazione nell'autofinanziamento aziendale. Se supportate da metodi e software mirati, permettono inoltre di analizzare i comportamenti della clientela; tramite la raccolta dati, infatti, è possibile effettuare studi sui loro acquisti nello spazio e nel tempo. Infine, aspetto da non trascurare, le gift card sono un ottimo strumento attraverso cui praticare la fidelizzazione.

Problemi associati all'utilizzo e limiti delle gift card

Naturalmente esistono alcuni aspetti per cui le gift card non si presentano come un mezzo sicuro per le transazioni. Innanzitutto, sono spesso soggette a smarrimenti o furti e, non essendo nominative, risulta difficile ricondurle al legittimo proprietario. Di conseguenza, in questo caso tutto il credito ancora disponibile sulla carta viene irrimediabilmente perduto senza la possibilità di ripristinarlo su una nuova tessera.

In secondo luogo, regalare una gift card permette inevitabilmente a chi la riceve di conoscere il valore del regalo, che risulta, oltretutto, freddo e impersonale. Inoltre, può capitare che al seguito dell'utilizzo della carta regalo, rimanga comunque una piccola somma di denaro insufficiente a procedere con un ulteriore acquisto, obbligando il possessore della carta a integrare con soldi propri oppure a perdere il credito residuo. Spesso, poi, le certe regalo non vengono nemmeno impiegate, in genere perché chi ne entra in possesso non gradisce la marca o il negozio presso cui è stata acquistata, oppure per mancanza di tempo, o perché viene smarrita ancora prima di essere utilizzata oppure ancora perché il negozio che l'ha emessa chiude.

Poiché una gift card viene in contatto con attori differenti lungo la catena distributiva (chi la rilascia - distributore - rivenditore - compratore - ricevente), non è raro che il codice riportato sopra la tessera venga compromesso, determinando un'esperienza non piacevole per il cliente e un danno per il commerciante. Ma fino a quando non viene riscattata, non è possibile capire che sia stata danneggiata e soprattutto per mano di chi.

Per quanto riguarda le cosiddette e-gift card, ovvero quelle carte regalo digitali acquistate online presso siti specializzati o direttamente da quelli delle aziende, si riscontrano spesso truffe e strategie fraudolente ai danni degli ignari acquirenti. Infatti, l'offerta allettante di gift card gratuite o la proposta convincente di compilare brevi moduli per ottenere sconti, inducono l'utente a seguire un link dopo l'altro fino a giungere in siti web fake che replicano quelli originali e a rilasciare dati personali di cui si servono i cybercriminali.¹⁰

Welfare aziendale

Una menzione particolare va fatta per l'impiego sempre più diffuso in Italia della gift card come metodo alternativo all'interno di un'azienda per distribuire benefit ai dipendenti. Negli ultimi anni, infatti, grazie alle normative vigenti¹¹, è possibile

¹⁰ Secondo quanto riportano gli esperti di Kaspersky Lab, <https://www.corrierecomunicazioni.it/cyber-security/siti-fake-e-false-gift-card-ecco-la-nuova-frontiera-della-truffa-online/>

¹¹ In particolare, articoli 51, 100 e 108 comma 2 del TUIR (Testo Unico delle Imposte sui Redditi)

raggiungere un certo livello di welfare aziendale che garantisce vantaggi ai dipendenti e ai datori di lavoro. Questi ultimi possono far leva su un'ottimizzazione del vantaggio fiscale e sulle agevolazioni disponibili, senza contare che curando il benessere dei propri collaboratori, il risultato percepito è quello di assicurare crescita e robustezza al proprio business. Al tempo stesso, ai dipendenti è assicurata la conciliazione della vita lavorativa con quella privata, nonché un aumento del potere di acquisto e, attraverso un miglioramento del clima aziendale, si favorisce la diminuzione di assenteismo e turnover.

In questo contesto si sta verificando una crescita importante dell'utilizzo delle gift card come strumento da affiancare alla classica retribuzione, per garantire il suddetto welfare aziendale. Infatti, si stanno sviluppando molte piattaforme che si occupano di offrire come servizio alle aziende la possibilità di acquistare voucher o gift card scegliendone il valore e la gamma di prodotti e servizi tra cui è possibile spenderli. Un esempio è costituito da Amilon, parte di ECRM Group e azienda leader in Italia nel digital rewarding, che, intuendo la possibilità di associare il proprio business alla soddisfazione di fringe benefit, ha creato la piattaforma Idea Shopping[®]. Questa consiste in un portale a cui si accede facilmente tramite una registrazione che permette di aggiungere al proprio wallet virtuale i codici Idea Shopping[®] e, successivamente, le gift card decidendone quantità e importo. In questo modo, chi beneficia del wallet può utilizzare il credito a disposizione scegliendo a piacimento gift card digitali tra le soluzioni offerte nel catalogo.

3.2 Loyalty Card

Cos'è e come funziona

La loyalty card o carta fedeltà è una tessera che consente di godere di sconti o premi, una volta che vengono conseguiti gli obiettivi predeterminati da chi la emette. Diffuse soprattutto nei settori come quello del retail (per esempio presso supermercati, negozi di abbigliamento o stazioni di servizio), le carte fedeltà vengono utilizzate con lo scopo di fidelizzare il cliente, in quanto danno accesso ai programmi di fedeltà per la promozione di particolari prodotti.

Una loyalty card consiste in una tessera di plastica solitamente nominativa che presenta una banda magnetica e un codice a barre. Una volta validata, entra in possesso dell'utente che la presenta al momento dell'acquisto presso il rivenditore o la catena che l'ha rilasciata. Per ogni unità di valuta di spesa, vengono accreditati dei punti sulla tessera in modo proporzionale secondo il regolamento della card stessa; quando vengono raggiunti determinati obiettivi prestabiliti, il cliente

ottiene un regalo che può consistere in un buono sconto oppure in un premio fisico.

Vantaggi

Per il cliente, il vantaggio più evidente è la possibilità di ottenere sconti o, in alternativa, un regalo fisico non necessariamente legato al settore o mercato dell'azienda che rilascia la fidelity card.

Ma i benefici maggiori sono registrati dalle aziende: come detto, la fidelity card è uno strumento connesso alle iniziative di marketing. Il fatto che la tessera sia nominale presuppone che il cliente sia stato registrato (almeno con i dati anagrafici principali) e che quindi l'azienda possa raccogliere tutte le informazioni circa le sue abitudini di acquisto come la frequenza, l'importo medio, gli articoli consumati. Poter conoscere le tendenze e le consuetudini dei propri clienti è la nuova frontiera nel rapporto con la clientela, perché permette di migliorare il servizio, stimolare un dialogo continuo con gli utenti, creare delle community di consumatori, incrementare le vendite e ottimizzare i ritorni degli investimenti.

Problemi associati

Il primo aspetto negativo è la necessità di avere fisicamente con sé la tessera al momento dell'acquisto, diversamente non risulta possibile caricare i punti ottenuti tramite la spesa.

In secondo luogo i punti accumulati presso un brand non possono essere riscattati presso un brand differente.

Ma la maggiore critica che viene mossa alle carte fedeltà da parte delle associazioni di consumatori è la mancanza di un reale risparmio. Ad esempio, ci sono supermercati che offrono ribassi fino al 10% della spesa una volta raggiunto un certo numero di punti, ma contemporaneamente spingono all'acquisto di prodotti più costosi per accumularli; altri, invece, scontano molto meno lo scontrino ma premiano gli affiliati con più offerte a scaffale. Inoltre, spesso, per ottenere i regali abbinati alle loyalty card è necessario raggiungere totali di spesa molto elevati e con integrazioni in denaro: facendo semplici verifiche si scopre come i premi in questione arrivino a costare tanto quanto li si pagherebbe comprandoli normalmente.

CAPITOLO 4

4. Studi di applicazione della blockchain alle gift card e loyalty card

4.1 Dati e statistiche sulle loyalty card

I programmi di fedeltà associati alle loyalty card attraggono sempre più il consumatore medio, che, in un primo momento, è spinto a sottoscrivere nuove iscrizioni da aggiungere al proprio "portafoglio" e, successivamente, è invogliato a mutare i propri comportamenti d'acquisto in modo da ottenere maggiori vantaggi dal programma di fedeltà a cui ha aderito; più precisamente il 66%¹² dei consumatori modifica l'ammontare speso per massimizzare i punti. Il funzionamento di questa strategia di marketing consiste nella massimizzazione della differenza tra il valore acquisito offrendo un programma avvincente e il costo di fornire i benefici associati a quel programma. Il passaggio chiave per un brand è quello di raggiungere la condizione di *lockin* per cui un cliente in una scelta tra due prodotti o servizi comparabili, predilige di default il marchio con il programma di fidelizzazione.

Ma quanto è importante per un brand offrire un buon programma di fedeltà? Attraverso il passaparola e l'interazione tra clienti, il 73% dei possessori di una fidelity card è propenso a consigliare una marca se ritiene che il programma di fedeltà a cui aderisce sia soddisfacente: è comprensibile, dunque, come chi si occupa di marketing ambisca a un risultato del genere.

La soddisfazione passa principalmente attraverso la riscossione dei punti, che gioca un ruolo cruciale: il 70% degli intervistati trova piacevole la possibilità di redimere i punti accumulati direttamente presso il negozio, con il 43% che afferma di essere disposto a pagare una quota supplementare a patto di ottenere immediatamente il premio che gli spetta. Da qui scaturisce un livello di soddisfazione 2,5 volte maggiore per chi riscatta punti rispetto a chi non l'ha mai fatto.

La chiave di tutto ciò sembra essere la personalizzazione: solamente il 22% degli aderenti a un programma di fedeltà trovano il livello di personalizzazione soddisfacente; quando il rapporto con il cliente permette di farlo sentire speciale o riconosciuto, si genera un'interazione emozionale che determina un aumento della

¹² Tutti i dati in questione presenti nel paragrafo fanno riferimento ai risultati dello studio Bond Loyalty Report 2016 condotto su 12.000 cittadini statunitensi e 7.000 canadesi attraverso questionari online.

fedeltà al brand e del livello di soddisfazione (2,7 volte rispetto a un programma standardizzato).

Sono, però, altri due dati a risultare estremamente interessanti: uno è legato al concetto di fiducia e l'altro alla tecnologia. Innanzitutto, con un dato in calo rispetto all'anno precedente, si registra che il 34% degli intervistati concorda pienamente sul fatto che i programmi siano fidati: decisamente una percentuale bassa se si considera che in media nei loro portafogli sono presenti 13,4 tessere-socio, di cui attive 6,7. In secondo luogo, poi, è stato analizzato il rapporto dei programmi di fedeltà con il mondo della tecnologia ed è emerso che il 49% dei rispondenti non sa se sia attiva un'app relativa al programma di cui fanno parte nonostante quasi tre persone su cinque vorrebbero interagire con il programma di fedeltà attraverso il proprio dispositivo mobile.

4.2 Ruolo della tecnologia blockchain

Queste informazioni permettono di comprendere perché, secondo uno studio condotto da Deloitte¹³, il futuro dei programmi di fedeltà e delle gift card è l'utilizzo della blockchain. In un contesto di scarsa partecipazione da parte dei consumatori, di mancanza di un sistema di gestione uniforme e di inefficienza dei programmi proposti dai brand appare evidente che un cambio radicale, come quello legato alla blockchain, potrebbe risolvere i problemi attuali e portare a un maggior guadagno sia per i consumatori sia per le aziende.

La soluzione potenziale, sarebbe, quindi quella di integrare programmi differenti tra loro in un unico network collegato, decisione che sarebbe impossibile senza un'adeguata struttura digitale alla base e senza le relative regolamentazioni per la gestione dei dati personali dei clienti e delle informazioni riguardanti il brand.

Presentandosi come un database distribuito che consente di effettuare transazioni in un nuovo modo mantenendo i dati in una rete sicura, trasparente, digitalizzata, interconnessa e che non necessita di fiducia, la blockchain permette di eliminare tutte le inefficienze che caratterizzano un programma basato su tessere; i partecipanti al sistema possono collegarsi tra loro e interagire senza bisogno di intermediari, ma soprattutto senza compromettere la propria privacy o la competitività tra aziende.

Secondo gli studi condotti, la blockchain consente la creazione, la riscossione e lo scambio istantaneo e sicuro di punti fedeltà tra programmi, venditori e aziende attraverso un ambiente trustless, utilizzando prove crittografiche al posto di terze parti e amministratori fidati. Tramite un rigoroso protocollo online, blocchi ben programmati e la connessione di smart contract, blockchain ha la capacità di

¹³ Deloitte. Making Blockchain real for customer loyalty reward programs

operare senza intermediari. Tutto ciò è possibile grazie a tre elementi fondamentali: piattaforma per la rete, applicazione disponibile per i partecipanti e loyalty token.

Il primo step è quello di creare una piattaforma che ospiti la rete di fidelizzazione: questa potrebbe coinvolgere diverse e molteplici organizzazioni e i loro programmi di fidelizzazione, facilitando la loro interazione, specialmente in termini di convertibilità e scambio dei loro punti.

In secondo luogo è necessaria la creazione di un'app che, tramite un portafoglio digitale, permetta l'accesso alla rete. L'app in questione contiene identità sotto forma di firme digitali, che memorizzano valore sotto forma di loyalty token. I fornitori di programmi possono gestire la loro app attraverso l'impostazione di alcuni parametri, in modo da conservare al meglio la propria competitività o strategicità di programma; in altre parole, controllano esattamente come i clienti accedono e riscattano i loro premi.

Infine, quando viene eseguita una transazione (emissione, riscatto o scambio), il protocollo blockchain crea un loyalty token generato da un algoritmo e che rappresenta una base per tutti i tipi di premi, inclusi i punti. L'esistenza del token e gli identificatori univoci sono aggiornati sul libro mastro di ogni partecipante e resi disponibili attraverso la rete.

Un interessante vantaggio che si può riscontrare nell'adozione della nuova tecnologia in questione è la riduzione dei costi. Inizialmente chi si occupa della gestione dei programmi di fedeltà, potrebbe esitare per il timore di incorrere in costi per l'implementazione di un sistema basato sulla blockchain; questa incertezza è comprensibile, dal momento che si tratta di modificare profondamente il modo in cui vengono eseguite transazioni, acquisizioni di clienti e gestione del sistema, ma è necessario guardare questi cambiamenti in un'ottica a lungo termine. Solamente in questo modo è possibile comprendere che un passaggio alla blockchain rappresenterebbe un'evoluzione e una semplificazione dello status quo, anziché essere una semplice sostituzione. Ovviamente l'implementazione della blockchain necessita di investimenti, ma è il trade off tra questi costi e il risparmio che ne consegue a risultare vantaggioso. Un esempio è dato dal fatto che per mezzo degli smart contract, sfruttati da questa tecnologia, si ottengono transazioni sicure, tracciate e vengono notevolmente ridotti i costi legati a errori o frodi.

Nell'ambito dei programmi di fidelizzazione, la riduzione di costi consente alle aziende di ridurre i requisiti di punti minimi ai quali i clienti sono autorizzati a riscattarli. La possibilità per i consumatori di utilizzare più rapidamente i punti aumenta le transazioni di rimborso, riducendo quindi i costi per singola transazione. Inoltre potendo implementare facilmente i programmi su piattaforme

di social media, anche i costi legati all'esposizione e alla sponsorizzazione sono ridotti.

Infine, un beneficio apportato dalla blockchain è la possibilità di eseguire operazioni e transazioni senza ostacoli dal momento che tutti gli attori si interfacciano con un'unica piattaforma che mette in condivisione le informazioni.

CAPITOLO 5

5. Le realtà presenti sul mercato: casi di studio

Per comprendere meglio il panorama delle offerte presenti attualmente sul mercato o in fase di lancio, è utile analizzare quali siano le proposte commerciali e, soprattutto, come risultino organizzate e strutturate le varie piattaforme o società fornitrici di servizi nell'ambito gift e loyalty card.

Ecco perché, di seguito, verranno presentati alcuni casi di studio esaminati con l'intento di comprendere come sia implementata la tecnologia blockchain all'interno di una realtà così specifica.

5.1 BitRewards

BitRewards si presenta come una piattaforma di premi e loyalty; il suo funzionamento prevede che i commercianti che aderiscono al progetto siano dotati in modo gratuito di un software chiamato BIT, utilizzato per premiare i clienti (per acquisti, Mi Piace sui social, condivisione con amici..) per mezzo di BIT token. Il circuito si compone quindi di monete reali e monete virtuali e sfrutta la tecnologia Ethereum.

L'idea di base è che il futuro della fidelizzazione sia segnato dall'utilizzo di registri distribuiti e protocolli blockchain.

Gli utenti traggono vantaggio dai premi che ottengono, poiché non dipendono dal successo economico del commerciante e possono essere scambiati con qualsiasi altro bene liquido; al tempo stesso i commercianti hanno la possibilità di gestire con più efficacia i programmi di fedeltà e di conseguenza migliorare le vendite.

Funzionamento

Quando un cliente procede con un acquisto online presso un rivenditore collegato al software di BitRewards ha la possibilità di vedere sia il prezzo espresso in moneta fiat, sia l'equivalente sotto forma di *reward* che può ricevere. Ogni cliente registrato nel sistema di fidelizzazione della rete BitRewards sul sito Web del rivenditore riceve automaticamente un cryptowallet con un indirizzo Ethereum unico; questo può a sua volta essere utilizzato per la ricezione e l'invio di Ether e / o di altri token.

I token BitRewards possono essere riscattati in qualunque momento: è sufficiente che il cliente stabilisca quanti BIT vuole spendere per un determinato acquisto e

l'importo dell'ordine viene ridotto a seconda dell'attuale tasso di mercato di BIT. Tutto il processo è regolato da uno Smart Contract che assicura che avvenga il corretto pagamento e lo scambio di valuta fiat e di BIT. Inoltre, il cliente può caricare BIT sulla rete BitRewards trasferendo e convertendo Ether dal proprio portafoglio.

Poiché è stato riscontrato che molti rivenditori non hanno ancora abbastanza dimestichezza con le criptomonete da utilizzare negli scambi, le operazioni possono essere svolte tramite l'operatore di BitRewards. Questo fornisce ai commercianti l'opportunità di effettuare transazioni in criptovaluta e utilizzare funzionalità di fidelizzazione della piattaforma, con l'intento di promuovere l'adozione di token BIT; il tutto accompagnato da un supporto di tipo legale, fiscale e contabile ai clienti.

Meccanismo di reward

Dopo che un cliente effettua un acquisto con i token BitRewards, il software BitRewards installato presso il commerciante invia all'operatore BitRewards una domanda detta "Richiesta di premi" (Figura 10). La richiesta contiene anche l'indirizzo e-mail del cliente (o altro ID) o l'indirizzo del suo portafoglio. Se l'operatore BitRewards riceve l'indirizzo del wallet, il sistema trasferisce i token dal suo stock al portafoglio. Se l'indirizzo è sconosciuto, l'operatore crea un nuovo account, vi trasferisce i token e il cliente riceve una notifica con i dettagli del portafoglio creato. Usando il link, il cliente installa il portafoglio web o mobile BitRewards, e può effettuare transazioni con esso, o scegliere di trasferire i propri token nell'altro portafoglio. Dopo il completamento dell'operazione, l'operatore della rete BitRewards produce una fattura in valuta fiat nell'indirizzo del rivenditore per l'importo che l'operatore ha speso per la transazione.

Pagamento di acquisti tramite l'operatore BitRewards

Nel caso in cui un cliente effettui un acquisto completo, o parziale, utilizzando token BitRewards, il rivenditore invia una richiesta tramite API per la vendita dei token. In risposta alla richiesta, l'operatore di rete restituisce il numero di conto bancario e l'importo in valuta fiat, che sarà pagato per la quantità di gettoni indicata. Dopo aver ricevuto i token, l'operatore trasferisce la moneta fiat al rivenditore. Utilizzando l'attuale infrastruttura di Ethereum, l'elaborazione delle transazioni può richiedere fino a 1 minuto.

Mantenimento delle riserve fiat e criptovalute presso l'operatore BitRewards

Per evitare brusche fluttuazioni dei tassi dei token BIT, viene creato uno smart contract di liquidità. Per il mantenimento del livello necessario di riserva BIT, delle valute legali o dell'Eth l'operatore BitRewards acquista o vende BIT sul mercato aperto o tramite lo smart contract di liquidità.

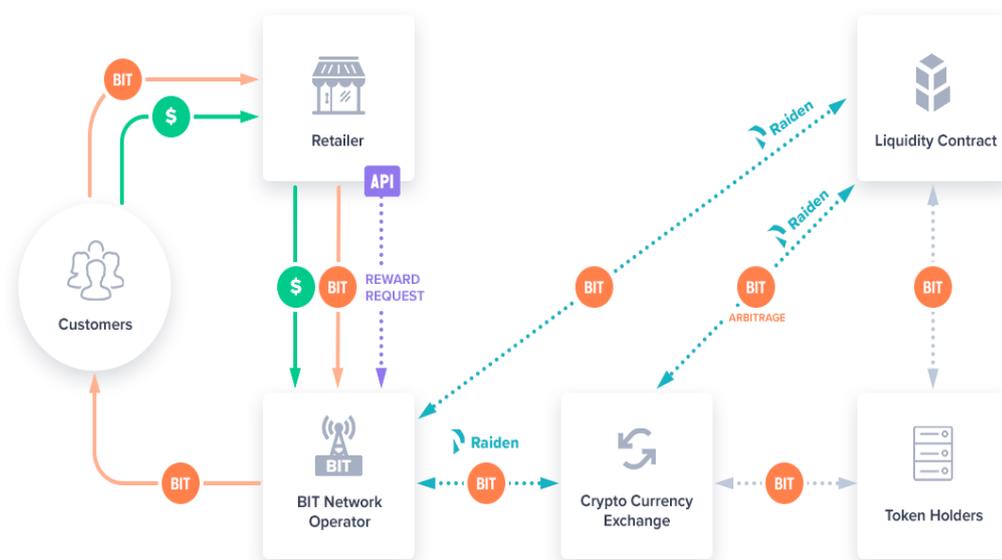


Figura 10 Rappresentazione grafica del meccanismo di reward, *BitRewards White Paper*

Smart Contract di liquidità

I token BitRewards sono progettati per aumentare di valore nel corso del tempo. I mercati delle attività crittografiche possono essere volatili e il prezzo del BIT può dipendere dalle condizioni e dalle aspettative generali del mercato. Poiché lo scopo principale del BIT è il mezzo di pagamento, è importante che il tasso del token rispetto alle valute criptate o fiat non cambi rapidamente e abbia liquidità in ogni momento. Per garantire questa condizione e attenuare le fluttuazioni, viene creato uno specifico Smart Contract, che consente l'acquisto e la vendita di BIT ed è utilizzato anche per aumentare la domanda e l'offerta del mercato. Lo smart contract di liquidità tiene una riserva di token del sistema BitRewards. Chiunque è in grado di acquistare o vendere BIT semplicemente inviando ETH all'indirizzo del contratto; questa soluzione è in grado di fornire la liquidità dei token e risolve il problema di una "doppia coincidenza di volontà", quando un acquirente e un venditore devono abbinare il tempo e il luogo in cui si verifica la transazione. Il contratto rispetta anche regole di mercato efficienti: al momento della vendita del bene, il prezzo scende, e al momento dell'acquisto del bene, il prezzo sale, quindi il contratto di liquidità cambia il prezzo di mercato del bene, disponibile per la

transazione, a seconda dell'importo applicato. Pertanto, la liquidità per qualsiasi parte interessata all'acquisto o alla vendita di BIT viene fornita in ogni momento.

Architettura di prodotto

I software per piattaforme di shopping online si presentano come widget da configurare all'interno del programma di fidelizzazione del rivenditore. Il sistema di premi e lealtà si basa su un insieme di soluzioni ampiamente applicate nell'e-commerce:

- uno strumento di "protezione del carrello": incentiva gli acquisti di completamento, che aumenta la spesa dei clienti e riduce la quantità di ordini abbandonati;
- un sistema di riferimento integrato con i social network;
- calcolatore del punteggio del promotore netto e modulo di revisione del cliente;
- soluzioni di carte regalo digitali, che consentono ai clienti di inviare carte regalo tramite e-mail, SMS, Facebook, ecc.;
- sistema di fidelizzazione basato sui punti: i clienti guadagnano punti per le loro azioni e i rivenditori possono definire quanti sono i punti corrispondenti in token BitRewards e a quale tasso di cambio.

Queste soluzioni sono trasferite sul DLT e sono fornite gratuitamente a tutti i membri della rete BitRewards (Figura 11).

Un altro strumento a disposizione dei rivenditori è la dashboard che viene impostata durante la creazione del programma fedeltà. Ciò consente ai commercianti di definire le azioni e l'ammontare dei premi guadagnati per il completamento di ciascun acquisto, inclusa la percentuale di acquisto restituita ai clienti per gli acquisti effettuati dai loro referenti.

Per quanto riguarda i clienti, questi possono iscriversi o accedere al programma di fidelizzazione tramite Facebook e altri social network, e-mail o telefono e ricevere accesso immediato al cryptowallet in cui possono vedere i BIT che sono stati aggiunti. I clienti possono accedere al portafoglio tramite il sito Web di qualsiasi commerciante di BitRewards Network o dal sito Web BitRewards. Il portafoglio BitRewards consente ai clienti di pagare con criptovaluta per gli acquisti da qualsiasi rivenditore sulla rete BitRewards. Il cryptowallet fornisce un unico indirizzo Ethereum al cliente e permette la memorizzazione, l'accettazione e l'invio di BIT, ETH e di qualsiasi altro token. Se l'ammontare equivalente al BIT supera i \$ 50 sul portafoglio del cliente, verrà offerto l'accesso all'autenticazione a due fattori (2FA) tramite Google Authenticator o SMS. Per impostazione predefinita, il cryptowallet memorizza le chiavi private sui server BitRewards Network in una forma crittografata. La chiave di crittografia viene creata dalla

chiave di accesso del cliente, con la quale accedono all'app BitRewards (Token di accesso di Facebook o Hash di password). La chiave può essere decifrata solo in presenza della sessione di accesso attiva del proprietario della chiave.



Figura 5 Rappresentazione grafica dell'architettura di prodotto, *BitRewards White Paper*

Tutto è strutturato in modo che il sistema impari attraverso l'esperienza a gestire l'enorme quantità di dati che provengono dai singoli rivenditori. I dati vengono immagazzinati in maniera decentralizzata sulla rete di Ethereum; questo tipo di struttura rende il sistema sempre operativo e disponibile per i clienti. Inoltre, se un rivenditore cerca di imbrogliare e invia dati falsi, viene rilevato e queste informazioni sono inviate alla blockchain di Ethereum.

Esiste anche la possibilità per i commercianti di vedere lo storico delle attività precedenti di ogni utente: infatti il sistema fornisce il punteggio circa la reputazione dell'utente, che consente agli esercenti di offrire un prestito o un pagamento posticipato per gli acquisti.

5.2 QiiBee

Partendo dai risultati di una ricerca condotta da Reuters & Affinity Capital Exchange (2017), secondo cui 500 miliardi di dollari sottoforma di punti non vengono riscattati dai membri dei programmi di fedeltà, QiiBee ha creato un sistema di fidelizzazione per marchi e brand che servono molti clienti; si propone di aiutare i marchi a gestire in pieno controllo i programmi loyalty sulla blockchain. Attraverso un solido protocollo, i brand hanno a disposizione gli strumenti per gestire e premiare la fedeltà dei clienti, per creare il proprio token di fedeltà e per coordinare le azioni del marketing. L'obiettivo è un software che permette la gestione dei programmi di fedeltà interagendo con la tecnologia blockchain per ottenere una maggiore efficienza e un'esperienza user-friendly.

Il brand che si rivolge a QiiBee crea la propria criptovaluta personalizzata attraverso il protocollo LoyaltyToken: stabilito il budget destinato al programma loyalty, può convertirlo in token di fedeltà, che vengono creati da QiiBee e inviati al cliente. Successivamente il marchio progetta in che modo distribuire i codici ai clienti (sullo scontrino, direttamente apponendoli sul prodotto, ...). Questi ultimi procedono con la registrazione online e l'apertura di un digital wallet in cui possono depositare i codici che ricevono: in questo modo ottengono l'equivalente in criptovaluta, che può essere spesa all'interno della rete di negozi del brand per acquistare oppure per ottenere dei reward. Al tempo stesso, il marchio in questione trae vantaggio dal coinvolgimento di clienti fedeli, senza contare la quantità di dati che può ottenere per monitorare tendenze e abitudini di acquisto.

Vantaggi per il brand

La caratteristica di essere un sistema *plug&play* è un vantaggio per il brand, perché questo mantiene il pieno controllo dell'interazione con il cliente: ad esempio, autonomamente determina come vuole premiare i suoi clienti fedeli e come vuole configurare il processo di riscossione dei punti.

In secondo luogo, aumenta il coinvolgimento che il marchio raggiunge poiché il valore dei suoi token non è fisso, ma subisce fluttuazioni che invogliano i clienti a detenerli per maggiore tempo.

Inoltre, viene mitigato il rischio di violazione dei dati, in quanto sono i clienti ad essere responsabili dei propri wallet.

Vantaggi per i clienti

Tramite app o accesso online al proprio digital wallet, ogni cliente è in grado di ottenere una panoramica di tutti i loyalty token raccolti da diverse marche

appartenenti alla rete QiiBee: infatti, il cliente può decidere se interfacciarsi con i singoli programmi di fedeltà oppure se importare tutti i token in un unico luogo comune. Poiché sono permesse transazioni, i token possono essere scambiati con altri clienti all'interno della rete QiiBee ed essere utilizzati per partecipare alle diverse offerte di riscossione dei vari marchi.

Inoltre, il fatto che tutti i token dei brand siano criptovalute legate al token QiiBee (QBX) quotato in borsa, implica che tutti i token posseggono un valore reale anche al di fuori del contesto del marchio e di conseguenza i clienti possono venderli per monete correnti o criptovalute tramite l'integrazione di terze parti.

Funzionamento

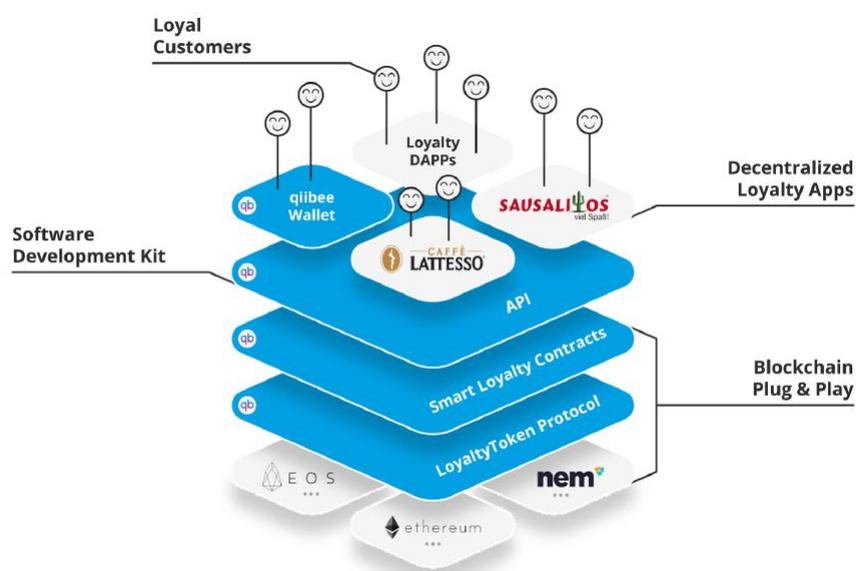


Figura 12 Rappresentazione grafica del funzionamento, *QiiBee White Paper*

Facendo riferimento alla Figura 12, si può avere una visione di come è impostato il sistema QiiBee. Al livello superiore ci sono i clienti fedeli, che utilizzano le app di lealtà decentralizzate. Un'alternativa attraverso cui possono interagire con il protocollo, è il digital wallet di QiiBee che comunica direttamente con la API (application programming interface) della rete; questa è il componente principale del *software development kit* e funge da ponte tra le singole app e il protocollo QiiBee, oltre a permettere ai marchi di creare e configurare i propri loyalty token. Infine, procedendo verso il basso, è presente il protocollo LoyaltyToken che consente la comunicazione tra Ethereum e le diverse catene di fedeltà utilizzate per i programmi di fidelizzazione dei brand; la base è rappresentata dall'infrastruttura blockchain. Questa è stata scelta perché fornisce un quadro ideale per affrontare i punti deboli del mercato della fedeltà di oggi: punti senza

un valore reale, programmi attendibili (debole privacy dei dati) e programmi di fidelizzazione altamente centralizzati.

L'SDK semplifica e facilita lo sviluppo di applicazioni in esecuzione sul protocollo LoyaltyToken, che consente di risparmiare tempo, denaro e un ampio know-how necessario per crearlo da zero. I brand possono concentrarsi sulle loro attività e sulle loro applicazioni, mentre vengono supportati tramite SDK. Più grande è la comunità che si basa sul protocollo QiiBee, più forte diventa l'ecosistema di lealtà offerto da QiiBee. Inoltre, è presente anche un dashboard interattivo in cui i brand senza fare affidamento su sviluppatori, possono facilmente impostare i programmi di fidelizzazione.

LoyaltyToken Protocol

Il protocollo fornisce una modalità fidata, sicura e dimostrabile per rilasciare token di fedeltà supportati da una risorsa crittografica attraverso diversi blockchain. Garantisce inoltre liquidità consentendo facili opzioni di riscatto, negoziabilità e uscita.

Il LoyaltyToken Protocol è basato su quattro componenti fondamentali: 1) una blockchain contenente un asset crittografico che supporta i token di fedeltà con un valore reale, 2) uno o più blockchain in cui risiedono i token di fedeltà, 3) un insieme di contratti di fedeltà che specificano come questi token di fedeltà sono, come si comportano e possono essere scambiati tra loro e 4) un ponte trasversale per abilitare la comunicazione crittograficamente sicura e il trasferimento di valore tra le varie blockchain.

Utilizzando i token QBX attraverso il protocollo fornito da QiiBee, i brand possono emettere token di fedeltà sulle diverse blockchain. Il token QBX attualmente opera sulla catena pubblica di Ethereum e la sua principale utilità è di agire come supporto per ogni loyalty token.

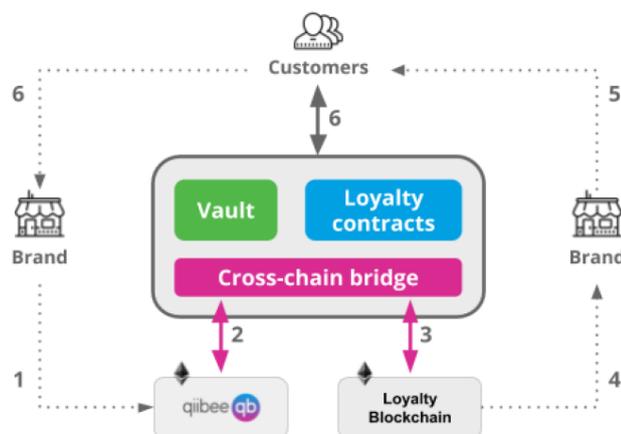


Figura 13 Rappresentazione grafica del protocollo, *QiiBee White Paper*

Il protocollo segue il flusso così composto (Figura 13):

- 1) Il brand acquista QBX sulla rete pubblica di Ethereum per emettere loyalty token.
- 2) Il cosiddetto *cross-chain bridge* blocca i token nel *vault*.
- 3) Il cross-chain bridge utilizza una comunicazione tra Ethereum e la Loyalty Blockchain per emettere i token di fedeltà.
- 4) I token vengono inviati all'account del brand.
- 5) Il marchio utilizza i token per premiare i propri clienti.
- 6) I clienti possono riscattare i token oppure scambiarli con QBX.

Per quanto riguarda le blockchain implementate, è stata costruita una catena privata basata su Ethereum che funziona in modo simile a quella pubblica e utilizza il meccanismo di consenso Proof-of-Work.

Considerando la Figura 14, si può notare che a sinistra è presente la blockchain pubblica di Ethereum, mentre a destra c'è quella privata.

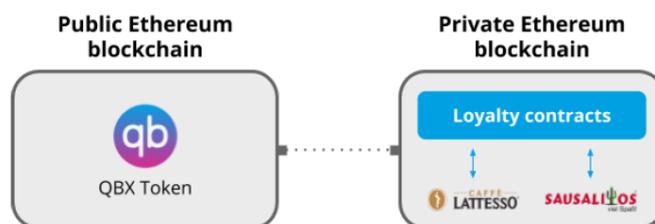


Figura 14 Configurazione delle blockchain coinvolte, *QiiBee White Paper*

L'estrazione di blocchi avviene solo quando viene eseguita una nuova transazione. Ciascuno dei nodi è incaricato di convalidare e confermare le transazioni in corso a seguito dei reward che i marchi danno ai clienti.

5.3 Tokky

Passando allo scenario delle gift card, Tokky si presenta come una piattaforma che vuole rivoluzionare il mondo delle carte regalo basandosi sulla blockchain, in modo da porre rimedio ai problemi che riguardano attualmente il settore.

Le problematiche che sono state riscontrate dai creatori di Tokky sono di diversi tipi:

- barriere all'ingresso per il settore: prerequisiti limitanti e vincolanti per chi vuole abbinare al proprio business un servizio di gift card, con difficoltà di gestione e elevati costi da sostenere;

- frodi e meccanismi complicati: la scarsa sicurezza permette frequenti furti di carte e spesso non vengono utilizzate o sono dismesse quando ancora contengono del credito residuo.

La soluzione proposta è quindi un sistema che permette l'utilizzo di carte regalo e carte ricaricabili multi-rivenditori senza gli inconvenienti appena citati. Inoltre, sfruttare la tecnologia blockchain comporta una serie di vantaggi come la rimozione del pagamento delle transazioni intermedie di servizio, l'immagazzinamento dei dati critici su un supporto immutabile e affidabile e, infine, transazioni che avvengono in modo automatico senza l'intervento di terze parti.

Funzionamento

Gli attori principali all'interno del sistema sono tre: le aziende che creano le carte Tokky, i promotori indipendenti che le distribuiscono e i clienti che le utilizzano (Figura 15).

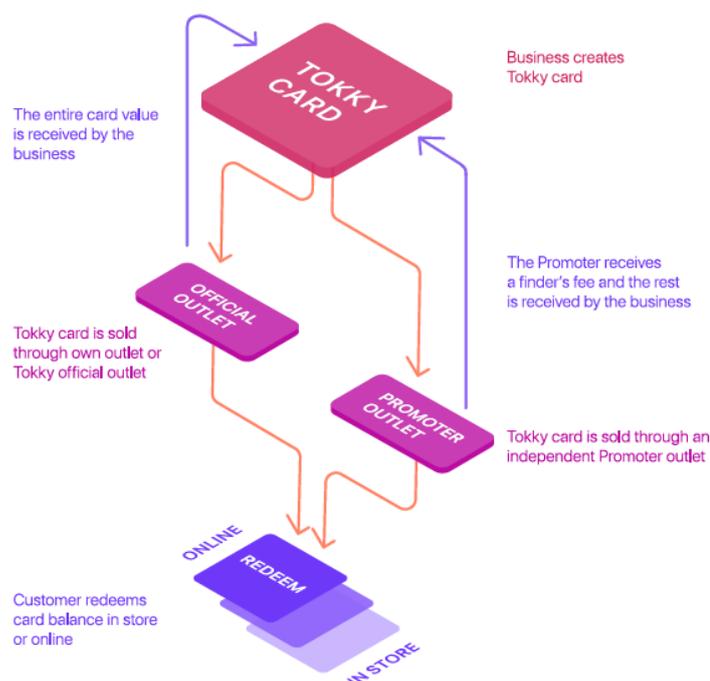


Figura 15 Rappresentazione grafica della piattaforma, *Tokky White Paper*

I primi sono aziende o individui che operano in vari settori di prodotti e servizi. Dopo aver stabilito il budget da dedicare al progetto, creano le carte Tokky che meglio si adattano alle esigenze e obiettivi del marketing. Queste vengono distribuite e vendute tramite i punti vendita di proprietà della società, oppure presso l'outlet Tokky ufficiale e i promotori indipendenti.

I *Promoter* sono aziende o individui che vendono le carte Tokky in modo autonomo e ricevono una commissione per ogni vendita; la struttura del sistema permette l'acquisto fisico e digitale.

Infine, i *Customer* o clienti, che possono accedere alla piattaforma tramite app o tramite sito web, acquistano le carte da impiegare per lo shopping personale oppure come regalo. Il saldo della carta può essere riscattato in negozio o online; in alternativa, i clienti possono rivendere le carte su un mercato secondario o utilizzare un'opzione di rimborso.

Per gestire il problema delle carte indesiderate o di quelle con un credito residuo basso che comporterebbero il tentativo di rivendita sul mercato secondario, Tokky ha ideato il concetto di *balance reuse pot*. Quando un utente ha un saldo della carta basso e inutilizzabile oppure vuole vendere una gift card poco gradita, può scegliere l'opzione che preferisce. In questo modo disabilita la sua carta mettendola in uno stato di *resale pending*, ovvero rivendita in sospeso; il credito viene trasferito nel "piatto di riutilizzo del saldo" in attesa che un altro utente acquisti una carta oppure che avvenga la ricarica del saldo da parte del brand in questione. Le transazioni sono regolate da Smart Contract che verificano l'esistenza di un eventuale saldo in sospeso e adempiono all'operazione. Il risultato finale è che l'utente che vende il saldo della sua carta ottiene il saldo sul suo conto come denaro utilizzabile per acquistare le carte Tokky da qualsiasi altro commerciante e, contemporaneamente, l'azienda che ha emesso la carta Tokky rivenduta riceve una commissione per consentire riutilizzo dei fondi da parte di un altro utente.

Esempio. 1. L'utente A acquista una carta del valore di 100 € ma ne utilizza soltanto 90.

2. A decide che non vuole spendere i rimanenti 10 €.

3. A segue le istruzioni sul portale e clicca sull'opzione "sell remaining balance".

4. Supponendo che la carta da 100 € fosse stata acquistata con uno sconto del 10% (e cioè che A avesse speso effettivamente 90 € per comprarla), il saldo che può essere venduto ammonta a $10\text{ €} - 10\% = 9\text{ €}$.

5. Al saldo viene sottratta una fee par al 5%, riducendo l'importo a 8,55 €.

6. Il bilancio di 8,55 € finisce nel *balance reuse pot* senza che avvenga nessun trasferimento di token o soldi, perché l'importo è già stato ricevuto dal commerciante che ha incassato la vendita della carta da 100 €. A questo stadio, A non riceve nulla in cambio per la sua cessione di credito.

7. A è segnalato come *sell pending* sul suo profilo.

8. L'utente B decide di acquistare una carta da 50 € presso lo stesso commerciante.

9. B paga 50 € e riceve la sua carta, senza venire a conoscenza dell'esistenza del *balance reuse pot*.

10. Al momento dell'acquisto della carta da 50 €, lo smart contract verifica se il *balance reuse pot* contiene del credito; in questo caso ammonta a 8,55 €: 41,45 €, quindi, vanno al commerciante mentre 8,55 € vanno sul saldo di A.
11. A si ritrova con un bilancio di 8,55 € che può utilizzare per il prossimo acquisto di carte Tokky da qualsiasi retailer.
12. Il commerciante ha ricevuto 41,55 € ed emette una carta di 50 € a B.

Architettura di prodotto

Tokky è un protocollo costruito sulla blockchain di Ethereum e che utilizza Smart Contract per l'emissione, la gestione e la rivendita di digital gift card. In cima al protocollo (Figura 16) vengono eseguiti i livelli di servizio e un insieme di applicazioni di terze parti che fanno uso dell'infrastruttura di protocollo e facilitano l'utilizzo dei suoi servizi.

Un livello del protocollo Tokky fornirà un'API che può essere utilizzata da qualsiasi sviluppatore per creare la propria app, sito Web o altra implementazione software, utilizzando i servizi e i dati disponibili sulla piattaforma.

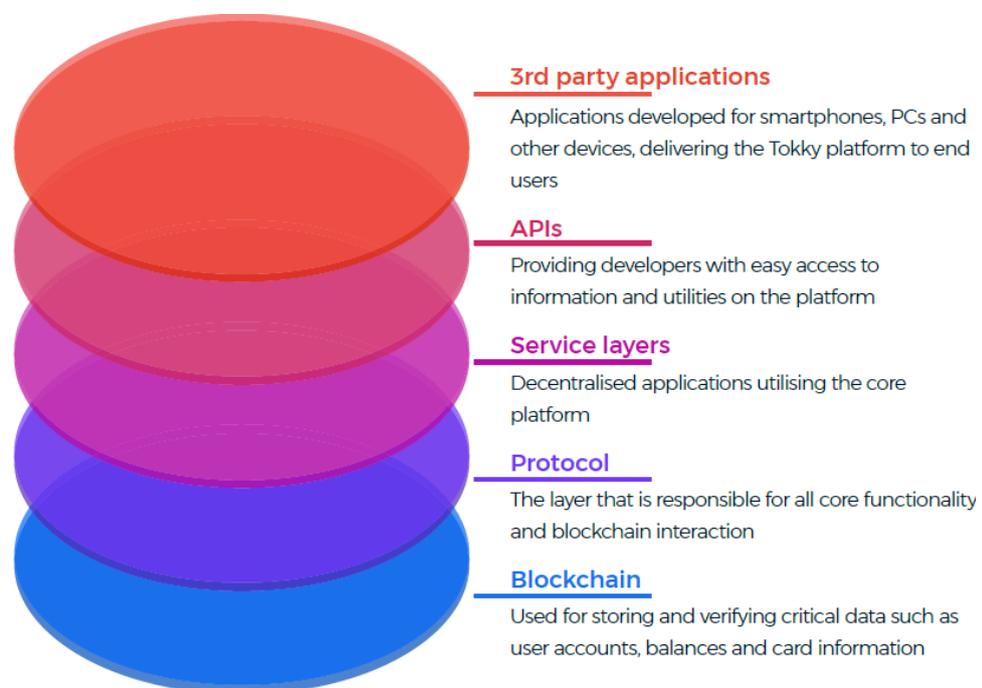


Figura 16 Rappresentazione grafica dell'architettura di Tokky, *Tokky White Paper*

La blockchain di Ethereum viene utilizzata per memorizzare dati critici come l'identificazione dell'utente e del commerciante, i modelli di carte emessi con tutti i termini e condizioni e la proprietà delle carte acquistate. I dettagli per ogni transazione originata da un pagamento con le carte Tokky sono archiviati in istanze di database distribuiti (in sola lettura e con dati accessibili solo tra l'utente e il commerciante), mentre i dati di prova e essenziali vengono archiviati sulla blockchain in formato hash.

5.4 Zeex

Zeex è una piattaforma di Zeek, società che da anni si occupa di vendere e scambiare gift card online; per realizzare la sua visione di rivoluzionare il commercio fondendo criptovaluta con il consumo quotidiano, Zeex propone tre concetti: Tap, Engage e Disrupt.

Tap fa riferimento al tentativo di superamento di un grosso ostacolo all'adozione e alla diffusione della criptomoneta: per renderla adatta ai pagamenti di beni e servizi quotidiani, Zeex permette che la criptovaluta sia facilmente convertibile in buoni regalo.

Engage implica l'integrazione di Zeex nei portafogli crittografici quotidiani dei clienti: poter spendere monete digitali al pari di altri metodi di pagamento, determina maggiore confidenza nelle criptovalute. Dal punto di vista dei commercianti, invece, il vantaggio risiede nella possibilità di accedere a dati critici di qualità, come le abitudini di acquisto e spesa dei clienti.

Infine, *Disrupt* con il significato di portare le gift card sulla blockchain: poiché le carte regalo sono un tipo alternativo di valuta, questa tecnologia può trasformare il loro uso e la loro distribuzione.

Alla base della soluzione di Zeex si trova il token ZIX, che offre tre funzionalità. E' prima di tutto un metodo di accesso alla piattaforma; poi, determina chi può eseguire una transazione e in che modo. Inoltre, elimina gli intermediari negli scambi coprendo il rischio transazionale. Tutto ciò è possibile grazie all'implementazione di Smart Contract all'interno del protocollo Zeex.

Il supporto di Zeek si rivela fondamentale in quanto garantisce l'accesso a un inventario di alta domanda per gli acquirenti di token iniziali: a un business già avviato e consolidato si aggiunge il concetto di trasparenza, immutabilità e decentralità che la realtà della blockchain si porta dietro.

Implementazione

Sebbene il concetto alla base della piattaforma Zeex - rendere scambiabili le criptovalute spendibili e le carte regalo - sia molto semplice, l'implementazione tecnica non è banale. In effetti, la realizzazione di questa idea comporta una serie di considerazioni commerciali e tecniche.

Come anticipato, la chiave per rendere la criptovaluta un metodo di pagamento efficace è il token ZIX. Questo presenta, tra le altre, una funzione di accesso alla piattaforma senza dover ricorrere ad altri servizi, come per esempio i social network, per evitare compromissioni di privacy.

In secondo luogo, il token agisce come un ticket di coda che permette l'accesso privilegiato a quelle carte con alta richiesta e determina la priorità nel caso di più contendenti.

Un metodo per ottenere sconti nello scambio con gift card è quello di tenere i token più a lungo possibile, in modo da conferire a ZIX un valore reale e misurabile.

Un'altra caratteristica di ZIX è quella di consentire a compratori e venditori di scambiare criptovaluta e buoni regalo direttamente con i token su Zeex fino al completamento della transazione e ottenere immediatamente la loro carta regalo. Gli utenti detengono i token per coprire il rischio posto dalla transazione; allo stesso tempo, impegnando i token su Zeex, Zeex fornisce il valore necessario per garantire la transazione fino al suo completamento.

Inoltre, il token permette di registrare le condizioni di mercato e le preferenze dell'utente: questo meccanismo per raccogliere i feedback, non garantisce solo vantaggio agli clienti, ma anche a Zeex stesso, consentendo un adattamento rapido e calibrato alle mutevoli condizioni del mercato e alle preferenze e ai profili dell'utente.

Il protocollo Zeex gestisce gli acquisti di gift card tra fornitori e acquirenti sulla blockchain di Ethereum, mantenendo riservati e sicuri i dati sensibili, come codici seriali e valori di verifica.

Inizialmente, Zeex verifica e approva i fornitori che stanno cercando di utilizzare la piattaforma Zeex. In seguito, i fornitori sono in grado di attingere in modo indipendente impegnando i token ZIX come garanzia. L'ammontare dei token ZIX da impegnare è basato sul volume degli scambi e sulla reputazione del particolare fornitore; i fornitori verificati vengono quindi aggiunti da Zeex all'elenco dei fornitori approvati sullo smart contract.

Prima di rifornire il loro inventario di carte regalo, i fornitori crittografano i dati sensibili contenuti nelle gift card con una chiave di crittografia specifica, denominata SwapKey. La chiave viene memorizzata pubblicamente sullo smart

contract e la sua chiave di decrittografia corrispondente viene mantenuta nascosta in modo sicuro, accessibile solo allo swapper di crittografia.

Quando un cliente procede con un acquisto (Figura 17), invia una richiesta di acquisto dettagliata (marca, valore nominale, ecc.), inclusa la chiave di crittografia unica, chiamata BuyerKey, e un pagamento sufficiente a coprire il costo della carta regalo e la commissione di transazione interna di Ethereum. Tramite uno smart contract, vengono verificati il pagamento e la disponibilità di una o più gift card dal valore nominale richiesto; una volta completato questo passaggio, la gift card è assegnata al cliente e il pagamento è trattenuto per il fornitore. Lo swapper di crittografia, un processo off-chain affidabile e isolato, analizza le transazioni di acquisto su blocchi appena estratti. Al rilevamento, decodifica la carta regalo assegnata con la chiave di decrittazione nascosta (la controparte di SwapKey) e la re-crittografa con l'appropriata BuyerKey. La carta crittografata viene quindi archiviata nello smart contract, che finalizza l'acquisto trasferendo il pagamento al fornitore emittente. La blockchain registra pubblicamente l'acquisto dell'utente, ma solo l'acquirente è in grado di decifrare e leggere il codice seriale e il valore di verifica della gift card.

Buyer sends purchase request:

- BuyerKey
- Brand name
- Face value
- Payment (cost, gas)

Swapper re-encrypts gift card:

- Decrypts with **secret key**.
- Re-encrypts with **BuyerKey**.
- Stores re-encrypted card on the smart contract.



Figura 17 Rappresentazione del processo di acquisto, Zeex White Paper

La tabella seguente riassume gli elementi rappresentativi delle quattro piattaforme prese in esame. Appare evidente come tutte e quattro rispettino le caratteristiche fondamentali per poter affermare di aver implementato alla base del proprio prodotto la tecnologia blockchain: sfruttano la rete di Ethereum, hanno sviluppato un proprio token agganciato all'andamento della moneta fiat e quindi dal valore fluttuante, utilizzano smart contract per l'esecuzione di contratti e, infine, impiegano i principi della crittografia come previsto proprio dalla blockchain.

	ETHEREUM	TOKEN	SMART CONTRACT	CRITTOGRAFIA	SUL MERCATO
BitRewards 	✓	✓	✓	✓	✓
QiiBee 	✓	✓	✓	✓	Fase di ICO ✗
Tokky 	✓	✓	✓	✓	✗
Zeex 	✓	✓	✓	✓	✓

Tabella 1 Caratteristiche delle piattaforme analizzate

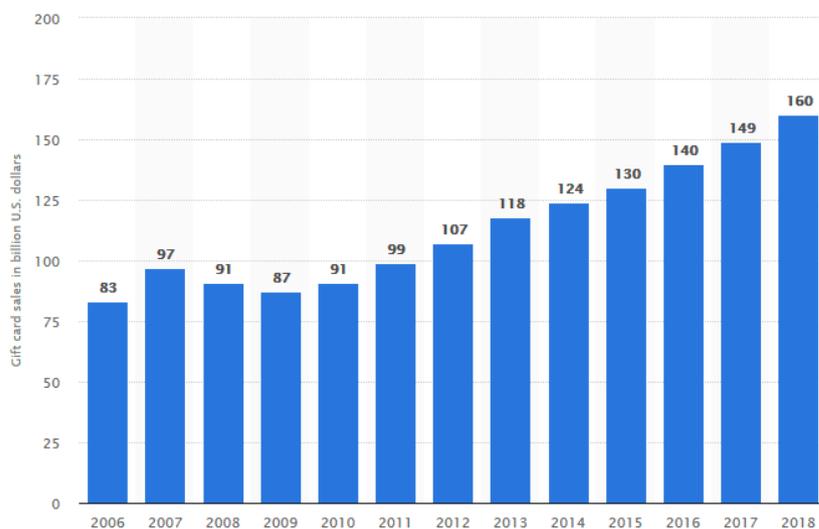
Come si può notare, BitRewards e Zeex sono già attive sul mercato perché si appoggiano a realtà esistenti da tempo (rispettivamente GIFTD e Zeek), quindi per gli sviluppatori è stato più facile proporre il servizio alla clientela. QiiBee e Tokky, al contrario, non sono ancora del tutto attivi, ma secondo le roadmap indicate nei rispettivi white paper, entro la fine del 2018 è previsto il loro lancio sul mercato: si tratta di testare le versioni beta dei software da presentare ai clienti, completare le ICO (Initial Coin Offer) per valorizzare i propri token e ultimare lo sviluppo di applicazioni accessorie.

5.5 Particolarità del mercato italiano

Le realtà analizzate non sono ovviamente le uniche presenti o in fase di lancio sul mercato globale, ma sono state selezionate per rappresentare le soluzioni proposte nell'ambito delle digital card: due di queste (BitRewards e QiiBee) offrono un servizio a supporto delle strategie di marketing attraverso l'implementazione di programmi di fedeltà che si basano essenzialmente sul digitale; invece, le altre due

piattaforme esaminate (Tokky e Zeex) garantiscono l'utilizzo della tecnologia blockchain a supporto della compravendita e dello scambio di gift card.

Il mondo digitale non conosce confini geografici, ma il luogo in cui vengono pensate e sviluppate queste realtà condiziona notevolmente il modo in cui vengono realizzate; considerando le quattro piattaforme prese in esame, queste sono nate in contesti in cui l'innovazione e lo sviluppo tecnologico sono favoriti e incentivati: Russia, Svizzera, Estonia e Israele. Il background di tipo culturale, economico, sociale ma anche quello legislativo, quindi, influenza inevitabilmente la struttura della piattaforma. Per esempio, si possono notare numerose differenze tra la società statunitense paragonata a quella italiana dal punto di vista dell'approccio alla tecnologia e dell'utilizzo di digital wallet: questo sicuramente si riflette anche sulla proposta di implementare la tecnologia blockchain in un ambito che in Italia è affrontato in modo diverso dagli USA. Mentre oltreoceano è molto diffuso l'utilizzo di gift card e loyalty card (Figura 18), in Italia questa abitudine non risulta così consolidata, anche se in forte crescita: da un'analisi svolta nel 2015 dall'Università di Padova, risulta che solo il 9% delle aziende intervistate utilizza gift card e che sono diffuse maggiormente nelle attività di incentivazione dei dipendenti (8,3% delle aziende intervistate le usa con questa finalità e il 12,5% dichiara che le userà nel prossimo futuro). Il potenziale di crescita del mercato delle gift card nel nostro Paese è dunque molto ampio, ma appare evidente come sia necessaria una politica di comunicazione dei vantaggi legati a questo strumento.



Data visualized by  + a b | e a u

© Statista 2018

Figura 18 Previsione di vendite di gift card negli Stati Uniti dal 2006 al 2018 (in miliardi di dollari USA), *Statista*

Intervista al CIO di Amilon

Questi dati si rispecchiano in ciò che è emerso da un'intervista rilasciatami personalmente da Renato Buontempo, CIO di Amilon, durante un incontro che mi ha concesso nel mese di ottobre 2018 presso la società di ECRM Group, che si occupa di soluzioni di digital reward e di prodotti e servizi di CRM e Customer Loyalty. Conoscendo bene il mercato italiano, Buontempo è stato in grado di svolgere un'analisi confrontando tra loro le realtà delle gift card e delle loyalty card e ha espresso il proprio parere, basato su studi condotti internamente alla società, circa la possibile implementazione della tecnologia blockchain.

Loyalty card

Partendo dalle loyalty card, è stato appurato che queste integrano uno o più programmi fedeltà che scaturiscono da precise direttive dell'area marketing di un brand: si stabilisce un budget, un obiettivo e le modalità di realizzazione; spesso, però, non avendo internamente le competenze tecniche, i brand si rivolgono a società terze, come può essere per l'appunto Amilon.

Oltre alle soluzioni individuali intraprese dalle singole marche, esistono da anni programmi "collettivi" che prevedono l'unione di aziende diverse, accomunate dall'utilizzo della stessa tessera. Un esempio di questa modalità di attuare programmi di fedeltà è rappresentato da Nectar. Nectar venne lanciata sul mercato inglese nel 2002 e fu presentata come uno schema di carte fedeltà a cui inizialmente aderirono quattro aziende; nel corso degli anni, poi, attratte dal successo che stava riscuotendo, si aggiunsero moltissime altre società appartenenti a settori differenti quali viaggi, vendita al dettaglio, finanza e editoria. Il funzionamento era semplice: attraverso l'acquisto presso i punti vendita delle marche aderenti, era possibile accumulare punti sulla tessera e riscattarli a piacimento per ottenere sconti oppure regali; tutti i punti confluivano in un unico conto legato alla tessera, di modo che fosse possibile usufruire di reward presso un determinato brand, anche se non tutti i punti erano stati accumulati tramite acquisti di prodotti o servizi di tale brand. In questo contesto, appare evidente come sia indispensabile un ente centrale che gestisca il meccanismo e che garantisca per le società coinvolte: oltre alla questione dei punti, le aziende erano attratte da Nectar per la possibilità di avere accesso a informazioni e dati riguardanti il mercato, raccolti proprio grazie all'utilizzo della card da parte dei clienti. E' quindi palese che non potesse essere una singola azienda a controllare il programma, ma qualcuno di esterno super partes. In Italia, una proposta come quella di Nectar incontra notevoli difficoltà di sviluppo a causa di vincoli burocratici, barriere e diffidenza di tipo culturale, ma soprattutto perché viene coinvolta una questione delicata, ovvero la gestione e lo scambio di dati riguardanti clienti: oltre a problemi legati alla privacy, si manifestano scetticismo

e sospetti radicati nella cultura italiana quando si tratta di condividere informazioni tra aziende non concorrenti tra loro.

Però, tralasciando la particolarità del contesto italiano, in un ambito come quello delle loyalty card, l'implementazione della tecnologia blockchain trova un suo motivo d'essere. La decentralità, il concetto di trust, l'immutabilità e la trasparenza sono caratteristiche che si sposano bene con i programmi di fedeltà di questo tipo. In alternativa alla scelta di affidarsi a una società fornitrice del servizio, i brand potrebbero accordarsi per sviluppare internamente e comunemente un sistema basato sulla blockchain.¹⁴

Gift card

L'intervista ha poi affrontato l'argomento gift card, che rappresentano forse l'ambito in cui Amilon e ECRM hanno maggior esperienza. Il primo commento emerso è stata la netta differenza per quanto riguarda la diffusione delle carte regalo rispetto agli Stati Uniti, come già evidenziato in precedenza. Se si considera il mercato italiano, inoltre, appare molto più consolidato l'utilizzo delle card all'interno delle aziende come strumento di welfare e per servizi ai dipendenti piuttosto che come offerta nel mondo retail. Questo disequilibrio nel rapporto tra B2B e B2C si riflette inevitabilmente anche nel business di Amilon che si trova maggiormente a fornire servizi nelle realtà aziendali: fringe benefit e altri strumenti di welfare, sempre più sovente, si appoggiano a strumenti come gift card, per la facilità di utilizzo e di gestione.

In uno scenario del genere però, l'opinione preponderante in Amilon non è favorevole al passaggio alla tecnologia blockchain: in seguito a studi e analisi interne condotte per capire quale fosse la strada giusta da intraprendere di fronte a un'innovazione tanto dibattuta e interessante, è emersa in primo luogo la difficoltà di implementazione, ma soprattutto è stato messo in discussione il ruolo della società stessa. Infatti, per Amilon, significherebbe passare su una rete gestita da terzi e verrebbe meno il discorso di *trust* che l'azienda, con il suo servizio, garantisce: basando parte del proprio prestigio sul ruolo di intermediario tra aziende e clienti attraverso l'emissione di gift card, è chiaro che perderebbe una fetta del proprio valore. La conclusione a cui è giunta la società è quella di considerare come valida alternativa, un investimento nel campo della sicurezza; anziché dedicare risorse per l'implementazione della tecnologia blockchain, al momento Amilon preferirebbe destinarle a un miglioramento dell'algoritmo a

¹⁴ In un contesto totalmente differente, si sta verificando un fenomeno paragonabile e inusuale: due colossi mondiali concorrenti tra loro nel settore dell'estrazione e del commercio dei diamanti hanno firmato un accordo che prevede lo sviluppo in collaborazione di una piattaforma blockchain per tracciare i diamanti e che sarà disponibile per tutti i player del settore. (Fonte: <https://www.ilbitcoin.news/quando-blockchain-mette-persino-daccordo-la-concorrenza/>)

protezione dei codici che contraddistinguono le card in modo da ottenerne uno più robusto.

Ovviamente si tratta dell'opinione di una singola società, che per storia, know-how, processi interni e mission, non può essere paragonata a nessuna altra realtà esistente: il giudizio conclusivo a cui è giunta Amilon deriva da discussioni e ragionamenti condotti al vertice della società, dopo una consultazione con la parte tecnica. Ciò non significa che in assoluto la blockchain non sia implementabile in un contesto di gift card o che Amilon non adotterà mai questa come soluzione: probabilmente al momento non si sono ancora verificate le condizioni essenziali per basare il business delle carte regalo sulla blockchain.

Conclusioni

Questa tesi ha avuto l'obiettivo di esplorare l'utilizzo della blockchain in un contesto ben preciso: quello delle carte regalo e delle carte legate a programmi fedeltà. In un mondo sempre più connesso, in cui la società sta attraversando un periodo di transizione dal punto di vista tecnologico, appare naturale interrogarsi sugli sviluppi di un'innovazione tanto dirimpente. Come ogni tecnologia rivoluzionaria, anche la blockchain sembra dotata della capacità di sconvolgere le abitudini e le pratiche affermatesi nel corso del tempo. Per poterne valutare gli effetti, però, è preferibile distinguere la tecnologia di base dalle sue applicazioni: ad esempio, non si può giudicare la blockchain attraverso le speculazioni collegate alle criptomonete, perché l'effetto di lungo periodo di questa innovazione trascende il suo legame con le valute digitali. Di blockchain e Bitcoin si è parlato tanto e non sempre nel modo più opportuno: negli ultimi mesi l'hype attorno a questo concetto è cresciuto notevolmente, tanto da renderlo una moda, una parola magica sulla bocca di tutti. Ma una tecnologia tanto complessa non è facile da interpretare e richiede un orientamento multidisciplinare: informatica, crittografia, implementazione di codici, teoria monetaria per citare alcune delle nozioni alla base della sua comprensione.

E' stata ritenuta fondamentale tale premessa, in quanto questa tesi non vuole in nessun modo valutare la tecnologia in sé, ma piuttosto analizzare se la sua applicazione in un ambito circoscritto e definito come quello delle card sia innanzitutto fattibile e, in secondo luogo, utile al fine di un progresso migliorativo. Per fare ciò, è stato indispensabile uno studio su più fronti: in principio la blockchain in sé, a partire dall'idea di Satoshi Nakamoto per arrivare al suo meccanismo di base, a seguire il mondo delle gift e loyalty card, e infine, le realtà presenti sul mercato.

A proposito di blockchain è stato molto utile leggere testi a più livelli, partendo da guide "for dummies", in modo da assimilare i concetti fondamentali, fino a giungere a documentazioni pensate per chi lavora con tali nozioni; alcune conoscenze pregresse mi hanno permesso di entrare più facilmente nell'ottica del funzionamento, ma la comprensione ha comunque richiesto tempo per essere acquisita. Subito dopo è iniziata una fase di analisi che in un primo momento prevedeva solamente le gift card, ma in seguito alla lettura di alcuni studi in cui comparivano le loyalty card, si è deciso di includere anche queste ultime nell'osservazione. Infine, si è resa necessaria una ricerca delle piattaforme presenti sul mercato che offrissero un servizio legato alla blockchain. Durante questa fase, si sono verificati numerosi contatti con professionisti del settore in occasioni

differenti tra loro e che hanno permesso di ottenere opinioni anche contrastanti circa l'utilizzo della blockchain nel mondo delle gift e loyalty card.

Una caratteristica che accomuna tutte le soluzioni prese in esame è senza dubbio l'utilizzo di una particolare blockchain, vale a dire Ethereum. La scelta sicuramente è dettata dal fatto che Ethereum permette lo sviluppo e l'implementazione degli Smart Contract, che si rendono necessari per permettere il funzionamento del meccanismo che regola le card. Infatti, il vantaggio che un qualunque utente ha di poter ottenere il proprio reward e accedere al proprio wallet contenente token diversi tra loro (nel caso per esempio di loyalty card) deriva appunto dall'impiego di questi contratti. Uno Smart Contract riceve informazioni che sono definite e certificate dalle parti del contratto stesso: una volta lette, le controlla e le interpreta sulla base di precise regole ed esegue le operazioni necessarie per ottenere l'output voluto. Trattandosi dell'esecuzione di un codice da parte di un computer, i dati sono elaborati in modo deterministico e si può garantire alle parti un giudizio oggettivo, poiché si esclude qualunque forma di interpretazione. Il fatto che le transazioni siano senza intermediari e dubbi interpretativi, rende il meccanismo più fluido e snello: non può che essere un vantaggio, soprattutto nell'ambito di gift card e loyalty card.

Una seconda evidente considerazione che scaturisce dall'analisi condotta durante la stesura della tesi riguarda l'origine geografica delle piattaforme: in linea generale ci sono dei Paesi che per cultura e predisposizione, favoriscono e assecondano la tecnologia, e quindi appare quasi scontato che siano la culla di soluzioni innovative che sfruttano la blockchain. In Italia si riscontra una sorta di diffidenza che determina ritardi nell'introduzione di nuove abitudini: in questo senso, non è stato facile trovare dati rilevanti di società che appoggiassero l'utilizzo della blockchain, specialmente se si considera che il settore di riferimento dell'analisi non è ancora completamente sviluppato (ma si riscontra un trend di crescita nell'ultimo periodo).

Un terzo fattore emerso durante lo studio delle piattaforme, invece, riguarda il loro grado di novità e innovazione. Infatti, bisogna distinguere tra società già esistenti che hanno un business costruito nel tempo, a cui si somma la tecnologia blockchain come integrazione del proprio servizio, e società, invece, che dal nulla offrono un'idea, una prestazione legata ad un concetto di gift card e loyalty a cui le aziende possono decidere di appoggiarsi. Nel primo caso rientrano BitRewards e Zeex, che si basano su realtà esistenti e consolidate a cui sommano l'implementazione della blockchain, mentre nel secondo si trovano le altre due società prese in esame, cioè Tokky e QiiBee che, essendo partite da zero, sono

ancora in fase di lancio sul mercato e si presentano come nuove realtà alla cui base lavora la blockchain.

In generale, le opinioni dei professionisti raccolte durante la scrittura di questo lavoro concordano nell'affermare che il mondo gift card e loyalty rientra in quei campi di applicazione della blockchain leggermente forzati, dove a far la voce grossa è più la componente di marketing e di pubblicità di innovazione che non il serio e concreto use case della tecnologia.

Questo per due ragioni principali: la prima è il problema della sicurezza del dato, dove oltre al timestamping, qualsiasi informazione inerente a un cliente o a un acquisto rientra in quel campo minato di dati sensibili soggetti prima di tutto a privacy stretta e inoltre a preservazione forte da parte dell'azienda; la seconda motivazione si riallaccia alla precedente, in quanto si potrebbe proporre l'utilizzo di un DLT privato per evitare le problematiche appena esposte, ma si perderebbe un po' il senso di decentralizzazione. In ogni caso, l'introduzione di token e soprattutto lo sviluppo di uno Smart Contract può risultare molto utile per una gestione automatica, decentralizzata e trasparente di tutti i rapporti e contratti interni al mondo gift card e loyalty, ma solo se implementato nel modo corretto, ovvero se completamente automatizzato; la semplificazione di gestione dei rapporti contrattuali raggiunge il massimo della sua efficienza, al pari con il senso di utilizzo, se non vi è traccia umana.

In conclusione, la blockchain appare tuttora più adatta ad applicazioni in altri settori, come per esempio supply chain, pagamenti cross borders, provenienza materie prime e contratti notarili. Questo però non deve costituire un freno nella ricerca di nuovi ambiti in cui lavorare con questa tecnologia; anzi, proprio per alcuni aspetti che attualmente rendono il sistema un po' rigido e meno adatto a certi contesti rispetto ad altri, stanno nascendo alcuni nuovi protocolli per rendere la blockchain un sistema ancora più versatile. Un esempio di ciò è costituito da Lightning Network che mira a migliorare la privacy in quanto le transazioni all'interno di un canale LN restano private, a implementare smart contract e a permettere di effettuare grandi quantità di microtransazioni immediate; sostanzialmente, LN si presenta come una sorta di infrastruttura con grandi potenzialità sulla quale sarà possibile costruire diverse tipologie di applicazioni.

Bibliografia e Sitografia

AA. VV., *BitRewards White Paper. Bringing blockchain to customers' loyalty*, December 30, 2017

AA. VV., *QiiBee White Paper*, 2018

AA. VV., *Tokky. The Gift Card Industry. White Paper*, 2017

AA. VV., *Zeex White Paper*, 2017

Arora A., *Method and System for Authentication of Coupons via Blockchain*, US 2018/0150865 A1, May 31, 2018

Bellini M., *Che cos'è e quali sono gli ambiti applicativi di Ethereum*, 30 agosto 2017, (<https://www.blockchain4innovation.it/esperti/cose-quali-gli-ambiti-applicativi-ethereum/>)

Berryhill J., Bourgerly T., Hanson A., *Blockchains Unchained: Blockchain Technology and its use in the Public Sector*, OECD Working Papers on Public Governance No. 28, June 2018

Bitcoin, <https://bitcoin.org/it/come-funziona>

Blockchain 4 Innovation, <https://www.blockchain4innovation.it/>

Blockchain, <https://blockchain.info>

Bond Brand Loyalty, *The 2016 Bond Loyalty Report*, 2017

Christopher Malmo, *One Bitcoin Transaction Consumes As Much Energy As Your House Uses in a Week*, 2017 (https://motherboard.vice.com/en_us/article/ywbbpm/bitcoin-mining-electricity-consumption-ethereum-energy-climate-change)

Coin Market Cap, <https://coinmarketcap.com/>

Comparini Avv. G., *La Carta Regalo ("Gift Card")*, Retail&Food, marzo 2015

Conoscenti M., *Blockchain: features and scalability*, Daiun Lunch Seminar, 2018

Consumer Reports, *Pros and Cons of Giving Gift Cards and Prepaid Cards. Cash may be king, but other options could be even better*, December 13, 2017 (<https://www.consumerreports.org/prepaid-cards/pros-and-cons-of-giving-gift-cards-and-prepaid-cards/>)

Deri O., *The Gift Card Industry Is Growing: Can Blockchain Facilitate The Growth?*, Benzinga, 29 giugno 2018

(<https://www.benzinga.com/markets/cryptocurrency/18/06/11959333/the-gift-card-industry-is-growing-can-blockchain-facilitate-th>)

Fromhart S., Therattil L., Deloitte Center for Financial Services, *Making blockchain real for customer loyalty rewards programs*, 2016

Grilli L., *Thesis: Card Rewards – A Realistic Use Case for Blockchain*, PaymentsJournal, 26 aprile 2018 (<http://www.paymentsjournal.com/thesis-card-rewards-a-realistic-use-case-for-blockchain/>)

Gupta M., *Blockchain for dummies*, IBM Limited Edition, 2017

Il Bitcoin.it, <https://www.ilbitcoin.news/>

Lingham V., Levitt M. et al., *Securing Digital Gift Cards With A Public Ledger*, US 2016/0267472 A1, Sep. 15, 2016

Lingham V., Levitt M. et al., *System and Method For Establishing A Public Ledger For Gift Card Transactions*, US 2016/0267605 A1, Sep. 15, 2016

Lingham V., Levitt M. et al., *Systems And Methods For Securing Digital Gift Cards With A Public Ledger*, US 2016/0267474 A1, Sep. 15, 2016

Naumoff A., *Works Like Magic: Blockchain to Help Streamline Loyalty Programs*, Cointelegraph, 26 gennaio 2017 (<https://cointelegraph.com/news/works-like-magic-blockchain-to-help-streamline-loyalty-programs>)

Pacino G., *Siti fake e false gift card, ecco la nuova frontiera della truffa online*, CorCom, 20 luglio 2018 (<https://www.corrierecomunicazioni.it/cyber-security/siti-fake-e-false-gift-card-ecco-la-nuova-frontiera-della-truffa-online/>)

Pedretti L., *Ethereum: Libro Bianco - White Paper*

Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008

Startup Business, <https://www.startupbusiness.it/tag/blockchain/>

Statista, <https://www.statista.com/>

Sule S., *The next level of gift card bundled with blockchain*, Blockchain Magazine, 27 marzo 2018 (<https://blockchainmagazine.net/next-level-of-gift-card-bundled-with-blockchain/>)

Swan M., *Blockchain*, O'Reilly Media, Inc, 2015