

ESAME CRYPTOCURRENCY E PAGAMENTI ONLINE

Argomento a scelta – COSA SONO LE MONETE DIGITALI, COME FUNZIONANO E A COSA SERVONO. CBDC E IL SUO SVILUPPO MONDIALE.

Le digital currency (o monete digitali) sono monete legali tracciate, memorizzate elettronicamente, basate sulla metafora teologica della Fiat money, ovvero della moneta fiduciaria, socialmente accettate sulla base di una promessa e della fede, anziché su un metallo.

La loro nascita viene datata oltre cinquant'anni fa dall'inventore di Visa, Dee Hock, poiché "semplificano" le modalità di pagamento: non hanno bisogno di essere cambiate alla frontiera, occupano meno spazio nel portafoglio rispetto a monete e contanti e offrono la modalità di pagamento a distanza e contactless.

A differenza delle virtual currency, nonostante abbiano entrambe un formato digitale, hanno uno status legale regolato e il loro rischio è legato a scelte individuali, piuttosto che strutturali.

Un esempio di moneta digitale emessa da una banca centrale è la Central Bank Digital Currency (CBDC), questa è una moneta con il medesimo funzionamento di una qualsiasi moneta o banconota; infatti, sono nate come loro monete complementari, offrendo l'opportunità di essere affiancate ad esse con un'alternativa digitale.

La CBDC non ha quindi una configurazione fisica, ma è ancorata a una banca centrale garantendone il valore nel tempo, poiché la sua volatilità è influenzata solamente dalle politiche monetarie e dal tasso di cambio.

Nonostante le sostanziali differenze, le banche centrali si sono ispirate alle cryptocurrency per la creazione delle loro Fiat Currency digitali, attraverso la tecnologia blockchain e le transazioni peer-to-peer.

La CBDC è una moneta pubblica e non elettronica privata, poiché, come già ribadito in precedenza non viene emessa da una banca commerciale, l'intento delle banche centrali è proprio creare un'alternativa al pagamento in contanti, i quali hanno un costo non indifferente legato anche alla sicurezza (hanno necessità di trasporto e immagazzinamento, sono più suscettibili a falsificazioni e furti), addirittura superiore a quello delle carte di credito e debito.

Lo sviluppo di un possibile Euro Digitale comporterebbe un azzeramento dei rischi di perdite causate da un fallimento bancario, poiché emesso da un'istituzione (le banche centrali) che non può fallire, mentre le banche commerciali sì.

Oltre a un risparmio di tipo economico, ha un risparmio in termini di tempo, consentendo un numero elevato di transazioni grazie anche a calcoli automatici.

L'infrastruttura di pagamento può configurarsi in due modalità: completamente centralizzata o parzialmente decentralizzata.

Nel primo caso, non sono previsti intermediari finanziari, è quindi compito della banca centrale occuparsi dell'emissione e della gestione degli spostamenti della moneta digital.

Al contrario, nel secondo caso, vi sono gli intermediari finanziari che ricevono una determinata quantità di moneta dalla banca centrale e devono occuparsi della loro distribuzione.

In entrambi le configurazioni, la novità sostanziale dalle tradizionali intermediazioni finanziarie, è la riduzione degli attori coinvolti e, di conseguenza, transazioni più rapide e commissioni minori anche su trasferimenti extra-nazionali (come già avviene con il progetto SEPA).

La CBDC consente alla banca centrale di "inviare" una serie di bit al posto di stampare banconote, sostituendo carta e metallo, garantendo la tracciabilità di tutte le transazioni che infatti vengono registrate e hanno bisogno di dell'identità del soggetto che le effettua.

Dal punto di vista del consumatore, il funzionamento della CBDC non sarà diverso da quello di un qualsiasi pagamento elettronico: nel wallet digitale sarà registrata una carta di pagamento per poter effettuare transazioni, proprio come la carta di credito o debito, ma non ci saranno commissioni aggiuntive.

La situazione cambia dal punto di vista dell'intermediario finanziario, che otterrà commissioni quasi azzerate, mentre l'esercente aumenterà il proprio utile netto.

Oltre agli aspetti economici e temporali delle CBDC, vi è anche un importante aspetto sociale nell'aumento di inclusione finanziaria di paesi più poveri fornendo servizi anche a coloro che non detengono un conto bancario o di deposito.

Lo sviluppo delle Central Bank Digital Currency ha interessato gran parte del mondo, la prima ad emetterla è stata proprio la Cina con l'e-CNY per contrastare il problema delle cryptocurrency che portano diversi problemi all'interno del paese.

Grazie all'e-CNY il regime autoritario cinese può tracciare e monitorare le transazioni, detenendo un controllo sull'andamento dei prezzi e applicando direttamente politiche monetari, ma soprattutto vengono facilitate le transazioni *cross-border* con il progetto in corso *m-bridge*, finalizzato a limitare le sanzioni imposte dagli Stati Uniti, che al contrario ha ancora molta strada da percorrere per la creazione di un dollaro digitale.

Negli Stati Uniti, già sono stati avviati studi sui rischi al fine di creare una moneta totalmente digitale, sicura e rapida nelle transazioni.

La progettazione allo sviluppo di una Central Bank Digital Currency segue lo stesso fondamento open source delle cryptocurrency, ossia una "Open CBDC" tramite il Project Hamilton nato dalla collaborazione tra Fed e il Mit di Boston.

Il problema principale allo sviluppo del progetto è la de-finanziarizzazione; infatti, negli Stati Uniti vi sono le più importanti banche commerciali del mondo

La diffusione di una CBDC americana comporterebbe non pochi problemi, perché ai correntisti converrebbe di più spostare i propri depositi sul wallet digitale controllato dalla banca centrale, piuttosto che in un conto bancario meno sicuro.

Per quanto riguarda l'Europa, ovviamente si sta già lavorando sulla struttura della CBDC europea: l'Euro Digitale.

Per il momento sono presi in considerazione due modelli differenti: modello account based, caratterizzato dalla presenza di un conto, e il modello token based.

Considerando l'attenzione e l'impegno dell'Unione Europea sulla questione della privacy, questa non può essere messa in secondo piano e il secondo modello è quello che verte di più alla sua protezione.

Entrambi i modelli hanno vantaggi e svantaggi e proprio per questo motivo, il coinvolgimento dei cittadini europei è essenziale nella scelta per comprendere le loro esigenze e aspettative.

La soluzione migliore sarebbe una via di mezzo tra i due modelli, garantendo la privacy e la maggiore flessibilità di programmazione del modello token based e la possibilità di effettuare maggiori transazioni grazie al modello account based.

Un caso più particolare è quello del Giappone, impegnati in diversi test per l'introduzione di una CBDC giapponese, ma non come obiettivo principale di politica monetaria; infatti, la popolazione giapponese non è interessata ad una valuta digitale, poiché ancora ancorata alla mentalità del contante.

I pagamenti elettronici sono aumentati negli ultimi anni, solo grazie alla crisi pandemica del 2020 poiché il pagamento in contanti era sconsigliato a causa dell'alta contagiosità del virus.

La BoJ sta cercando una soluzione per garantire una rete sicura di pagamento facilitando le transazioni anche in caso di catastrofi naturali che spesso si riversano sul paese essendo in una zona ad alto rischio sismico. Se riuscisse a rendere lo yen digitale usufruibile in ogni contesto, anche in casi danni alle infrastrutture elettriche, i cittadini sarebbero disincentivati all'uso dei contanti perché riterrebbero la nuova moneta digitale molto più sicura.

2) DESCRIVERE LE DIFFERENZE FRA CRYPTOCURRENCY E LE MONETE COMPLEMENTARI

Le monete complementari sono nate con il fine di creare una diversa alternativa al tradizionale metodo di pagamento, completando il sistema monetario per sanare eventuali insufficienze. La nascita delle monete complementari viene corrisposta a John Maynard Keynes, il quale ha pensato ad una moneta chiamata *bancor*, prendendo ispirazione dalla moneta bancaria. La sua ipotesi non venne presa in considerazione durante la conferenza di Bretton Woods nel 1944, ma fondò le basi del sistema monetario internazionale e consentì una crescita esponenziale dell'Unione Europea nell'ambito del pagamento per raggiungere uno spazio comune economico. Keynes ipotizzava la Clearing Union come una banca e i correntisti come i vari paesi membri. La *bancor* fungeva da unità di conto per le transazioni, ogni paese (ossia i correntisti) deteneva un'apertura di credito pari alla somma delle loro esportazioni e importazioni. Le transazioni avvenivano grazie ad un sistema di compensazione, per cui il conto degli esportatori risultava positivo ad ogni transazione e quello degli importatori invece negativo.

A differenza di una banca commerciale, la Clearing Union non aveva bisogno né di depositi, né di capitali, né di riserve, poiché i correntisti potevano effettuare esclusivamente operazioni commerciali e non consentiva la conversione del compenso in valuta ufficiale.

Gli interessi venivano pagati da entrambi, sia da debitori che da creditori, sottolineando un'altra differenza tra Clearing Union e una banca commerciale, gli oneri erano uguali per entrambe le parti, consentendo l'equilibrio del saldo uguale a zero.

Non di rado le cryptocurrency come i bitcoin vengono intese come monete complementari, in grado di essere affiancate alla moneta tradizionale, ma a dire il vero le differenze sono sostanziali e in primo luogo poiché le cryptocurrency nascono con l'intento di sostituire i tradizionali modi di pagamento in ogni ambito, infatti sono *alternative coins*. Queste si fondano sulla competizione e il loro fine è proprio la sfida alle istituzioni; infatti, non sono regolate da nessuna autorità, si basano esclusivamente sulla difficoltà del loro criptaggio, cercando in tutti i modi di evitare comportamenti negligenti. Le cryptocurrency come conseguenza alla loro competizione seguono un modello gerarchico tra chi le possiede e chi no, a differenza delle monete complementari.

Inoltre, la tecnologia delle criptovalute è basata su una tecnologia blockchain con algoritmi crittografici finalizzati a garantirne la sicurezza, mentre le monete complementari si basano su sistemi diversi e non per forza sulle blockchain

le criptovalute sono progettate per operare su scala globale e possono essere utilizzate da chiunque abbia accesso a un dispositivo e a Internet mentre le monete complementari, invece, hanno un ambito di circolazione circoscritto, spesso legato a una specifica comunità o territorio. Vi è una grande differenza riguardante la loro finalità di utilizzo, in quanto le criptovalute sono principalmente utilizzate come mezzi di scambio digitali e come forma di investimento, concepite come alternative alle valute tradizionali, offrono la possibilità di effettuare transazioni globali in modo rapido e sicuro.

Le monete complementari, d'altra parte, sono create per promuovere scambi all'interno di una specifica comunità e per soddisfare bisogni locali, svolgono la funzione simile a quella del baratto e si basano sulla reciproca cercando di favorire lo svilupparsi di attività produttive.

L'ultima rilevante differenza è la modalità di emissione e gestione, da una parte le cryptocurrency si creano attraverso processi di mining e quindi l'emissione è decentralizzata, così come la loro gestione varia a seconda della criptovaluta di riferimento, il valore delle criptovalute è altamente volatile e la loro liquidità dipende dalla disponibilità degli acquirenti sui mercati.

Al contrario, le monete complementari nascono da istituzioni e hanno un corso legale, riconosciuto ugualmente da tutta la comunità e il loro valore rimane stabile.

3) DESCRIVERE RUOLO E COMPITI DEGLI SMART CONTRACT;

Gli smart contract sono letteralmente dei “contratti intelligenti”, ossia dei software utilizzati sulla blockchain per automatizzare l’esecuzione di un accordo tra le parti, in modo tale da far seguire le condizioni, garantendo sicurezza e autenticità, eliminando gli intermediari e di conseguenza risparmiando tempo.

Sono costituiti da un codice crittografico e servono da garanzia per far sì che il contratto tra le parti venga rispettato. Una volta che uno smart contract viene creato, si ha un codice contenente tutte le indicazioni e le condizioni di esso (prezzo, scadenze, quantità...) che viene caricato sulla blockchain consentendo l’automazione delle funzioni ogni volta che le condizioni vengono soddisfatte, di conseguenza non c’è la possibilità che non si adempia al compito, perché è tutto automatizzato. Inoltre, sono immutabili; quindi, quando vengono sanciti non possono più essere modificati e questo li differenzia dai tradizionali database, ma allo stesso modo possono gestire affidabilmente un’alta mole di dati.

Essendo open source sono consultabili da tutti prima di utilizzarli e il fatto che non vengono coinvolti intermediari e che i dati delle transazioni sono condivisi riduce al minimo la manipolazione egoistica da parte di una delle parti, per sfruttare gli accordi a proprio vantaggio.

Esempi in cui vengono utilizzati gli smart contract è durante il processo automatizzato di trasferimento di fondi, oppure per garantire l’autenticità degli NFT (Non Fungible Taken) o anche per verificare l’identità digitale riducendo frodi grazie al suo utilizzo sulla blockchain.

Gli smart contract si posizionano contemporaneamente su tutti i nodi di una blockchain; infatti, il loro costo dipende proprio dai criteri che questa adotta.

Gli smart contract possono interagire tra loro, ma hanno maggiori difficoltà a interagire con le informazioni esterne alla blockchain poiché ne sono solamente all’interno, di conseguenza per aspetti esterni alla blockchain, siamo costretti a affidarci a fonti esterne, denominati “oracoli”, ossia programmi esterni che danno informazioni su eventi esterni alla blockchain, come ad esempio il meteo o il valore di un’azione.

Gli oracoli forniscono informazioni in tempo reale, che possono poi essere utilizzate dagli smart contract per prendere decisioni, ma bisogna tenere in conto che ciò che sta all’interno della blockchain deve fidarsi delle informazioni che arrivano dall’oracolo, in quanto non sono comunque verificabili.

Giuridicamente parlando, il Ministero dello Sviluppo Economico italiano ricorda che è raccomandato avviare sperimentazioni volte alla possibilità di digitalizzare flussi di lavoro che implementano servizi in forma di smart contract, in modo da massimizzare la trasparenza, l’accessibilità da parte degli utenti, l’interoperabilità con altri servizi, l’apertura selettiva dei dati. Grazie a espedienti tecnici denominati DLT Oracle (oracoli dei registri distribuiti). Esemplicando l’esperienza di un volo aereo, grazie agli DLT Oracle, lo smart contract in questione può quantificare il ritardo del volo, la sussistenza, e quindi procedere in automatico al rimborso. Dunque, una volta validato, lo smart contract viene distribuito all’interno di un blocco della DLT e una volta avvenuto ciò non sarà più modificabile. L’ultima fase è il completamento, dove vengono sbloccati i fondi vincolati proprio per permettere l’adempimento del contratto.

Gli smart contract, come già detto in precedenza, sono programmati per eseguire operazioni su dati immutabili all’interno della blockchain, che li rendono estremamente sicuri e affidabili.

Quando un contratto viene creato sulla blockchain, viene immagazzinato in un registro immutabile che può essere visualizzato e verificato da chiunque.

Gli smart contract sono strettamente collegati alle applicazioni decentralizzate (DApp), ovvero programmi eseguiti sulla blockchain che consentono agli utenti di accedere a servizi e funzionalità in modo completamente decentralizzato e autonomo e possono essere utilizzate in vari settori, come ad esempio per la creazione di mercati decentralizzati finalizzati alla compravendita di beni e servizi in sicurezza.

Le DApp rappresentano un'importante innovazione nel campo dell'economia decentralizzata, eliminando la necessità di intermediari.

Queste due innovazioni tecnologiche (gli smart contract e le DApp) stanno trasformando il sistema fiduciario, passando da istituzioni centralizzate a sistemi matematici e crittografici, implementando la trasparenza delle operazioni,

Il consiglio nazionale del notariato guarda al momento con sfavore agli smart contract, in quanto gli viene riconosciuto un ruolo significativo ma non autonomo. Questo perché servono delle linee guida dell'AGID (Agenzia dell'Italia Digitale), affinché possa dirsi in maniera inoppugnabile che lo smart contract soddisfa il requisito della forma scritta, e per avere degli standard condivisi in relazione alla condizione delle parti. Al momento mancano ancora dei tasselli normativi per permettere agli smart contract di diventare più importanti nel nostro sistema giuridico.

4) DESCRIVERE LE MODALITÀ DEI PAGAMENTI ONLINE.

I pagamenti possono essere effettuati con differenti modalità, sono utilizzati per l'acquisto di beni o servizi e per trasferire denaro garantendo la corretta esecuzione.

Gli attuali metodi di pagamento possono essere divisi in Paper based payment (contanti, assegni e bonifici) e digital payment (e-money, carte e sistemi di pagamento alternativi), in base alle parti coinvolte, alla modalità, alla velocità della transazione, alla zona geografica, al canale di pagamento, al valore in questione e ai volumi.

Partendo dall'e-money, questa è testualmente la "rappresentazione della valuta a corso legale, il cui saldo è convenzionalmente visto tramite applicazioni (e-wallet) che ne custodiscono il valore". È una moneta elettronica come credito nei confronti della banca emittente salvato su un dispositivo elettronico. In questo caso, i fondi per l'emissione della moneta non sono un deposito per il cliente e ne consegue che la banca non ha interessi su questi fondi.

In Italia e nell'Unione Europea gli unici istituti autorizzati a emettere moneta elettronica sono le banche e l'IMEL (Istituto di Moneta Elettronica).

L'utilizzo può avvenire con carta di pagamento (prepagata) o tramite applicazioni digitali (wallet). Gli strumenti della moneta elettronica possono essere ricaricabili o non ricaricabili, co-branded o standard.

In base alle disponibilità del titolare, questo potrà rimettere fondi sulla sua carta oppure no e disporre di una carta fisica o digitale.

Se la carta è ricaricabile, il Titolare dello strumento di moneta elettronica potrà ricaricare lo strumento tramite bonifico bancario da un conto corrente bancario, oppure con un versamento in denaro contante presso un punto vendita abilitato, oppure negli altri modi messi a disposizione dall'istituto emittente.

la moneta elettronica potrà essere spesa presso esercenti convenzionati poiché è necessario il corrispondente circuito di appartenenza della carta e non potrà superare il limite della sua disponibilità.

Il titolare potrà in qualunque caso visionare le sue transazioni e conoscere il suo saldo disponibile e richiedere il rimborso del saldo in avanzo presente sullo strumento.

Il pagamento con carta elettronica è quello di più recente e larga diffusione, sia per gli acquisti offline che on-line. Le carte elettroniche sono generalmente tessere plastificate con un codice di riconoscimento e si differenziano in carte di credito, debito e prepagate.

Le carte di credito possono essere rilasciate da una banca o da una società emittente secondo un contratto che limita l'utilizzo solamente agli esercenti convenzionati, così come il loro prelievo di contante (presso ATM). Prevedono un anticipo di contante, conseguendone il pagamento di un interesse generalmente, che poi verrà pagato dal titolare della carta in un momento successivo. Per possedere una carta di credito si devono soddisfare determinati requisiti, ossia essere un cittadino europeo o viverci da almeno 3 anni, avere un'età compresa tra i 18 e i 70/75 anni, avere un reddito e un conto corrente attivo.

I soggetti della transazione sono quattro: l'issuer (emittente della carta), acquirer (banca dell'esercente che gestisce la transazione), Merchant (esercente convenzionato) e il circuito di pagamento (reti di pagamento come Visa, Mastercard, American Express).

Le carte di debito prevede l'addebito immediato dell'importo delle transazioni sul conto corrente; infatti, viene emessa a una banca ed è collegato ad un conto corrente bancario. Erroneamente in

Italia viene chiamato "bancomat" che in realtà uno dei circuiti che consente le transazioni nazionali, che insieme ad altri circuiti come Mestro, Mastercard Debit o Visa Debit consentono le transazioni internazionali. Infatti, la maggior parte delle carte di debito sono finalizzate anche per un uso internazionale.

Infine, la carta prepagata consente di utilizzare determinate somme di denaro per i pagamenti in base al credito che gli viene caricato, può essere effettuato tramite bonifico, con un versamento in contanti o direttamente automatizzato come addebito sul conto corrente.

In un pagamento con carta elettronica, ci sono diversi passaggi, attori e una catena del valore che consentono l'elaborazione e l'autorizzazione della transazione. Il consumatore seleziona il prodotto o servizio che desidera acquistare e il cassiere inserisce l'importo dell'acquisto nel terminale di pagamento o POS (Point of Sale). Il cliente presenta la propria carta di credito o di debito al terminale di pagamento che comunica con la banca del consumatore attraverso la rete di pagamento, la banca del consumatore conferma che il conto del consumatore dispone dei fondi sufficienti per coprire l'acquisto e ne autorizza la transazione e comunica l'autorizzazione al terminale di pagamento. Infine, il terminale di pagamento stampa la ricevuta di pagamento e il consumatore firma la ricevuta o inserisce un codice PIN per confermare l'autorizzazione della transazione. Il terminale di pagamento invia i dettagli della transazione alla banca del negoziante che accredita il pagamento sul conto del negoziante.

In tutto ciò, le reti di pagamento come Visa, Mastercard, American Express e altre svolgono un ruolo chiave nella gestione delle transazioni elettroniche, consentendo alle banche di comunicare tra di loro e di elaborare le transazioni in modo sicuro ed efficiente.