fondazione olitec

SCHEDA DI SINTESI REALIZZATA PRO BONO PER L'ANALISI DELLA FINANZIABILITA' DI APPLICAZIONI FACENTI PARTE DELLA CATEGORIA METAVERSO (VRO) PER SIMEST – CDP – MAECI

Ministero degli Affari Esteri
e della Cooperazione Internazionale

simest
gruppo cdp

cdp

Massimiliano Nicolini

DIPARTIMENTO DI RICERCA E SVILUPPO Roma

Sommario

Olitec ®© Laboratorio di Ricerca e Sviluppo presso
Fondazione Olitec Caritate Christi - olimaint©® is a trade mark of Olimaint Company
Brescia Via Saleri 55/58 - Italy (EU)
Valmontone via Colle S.Angelo 2/O - Italy (EU)

www.olimaint.tech - desk@oliverso.it

☏ +39 030 364332 int 5 +39 345 563 0496

fondazione olitec

OLIMAINT informatica e telecomunicazioni

olitec

SCHEDA DI SINTESI PER L'ANALISI DELLA FINANZIABILITA' DI APPLICAZIONI FACENTI PARTE DELLA CATEGORIA METAVERSO (VRO) PER SIMEST – CDP – MAECI

Quadro tecnico normativo specifico internazionale di riferimento

Le applicazioni di VRO (metaverso per usi socioeconomici) basano la loro natura tecnica sull'applicazione di otto principi che sono alla base della veridicità per confermare la caratteristica tecnica tipica della virtual and room object technology.

L'utilizzo della tecnologia VRO è particolarmente indicato per la realizzazione di piattaforme che permettano alle imprese di poter interagire virgola in una forma molto evoluta, attraverso uno strumento digitale con potenziali interlocutori in tutto il mondo; voi la particolare versatilità della programmazione della realtà immersiva permette di riprodurre di ricostruire un ambiente all'interno del quale possono essere messi in funzione tutti i sistemi di processo e le modalità operative tipiche e proprie dell'incontro reale tra fornitore e cliente ovvero tra colui che propone è colui che valuta la proposta.

Per poter valutare in maniera approfondita è corretta se un progetto rientra tra le specifiche tecniche minime per essere considerato un progetto di realtà immersiva o di metaverso è necessario analizzare nel dettaglio la struttura funzionale dell'applicazione seguendo una lista di controllo che permette di monitorare e di verificare in un lasso di tempo molto veloce se l'applicazione è meritevole di essere annoverata tra le applicazioni reali di metaverso o se invece è un'applicazione che cerca di assomigliare ad un'applicazione di metaverso.

La matrice fondante delle applicazioni di metaverso è l'interoperabilità, anche a breve termine, fornendo l'opportunità di condividere esperienze, approfondimenti e feedback su molteplici casi d'uso e piattaforme che saranno essenziali per lo sviluppo di un economia creatrice aperta ed equa.

Le esperienze del metaverso verranno create una volta ma distribuite su una varietà di piattaforme, quindi dovranno essere conformi alle capacità di specifiche piattaforme di destinazione per prestazioni ottimali massimizzando al contempo la fedeltà visiva all'intento del creatore.

Prevediamo che le parole virtuali siano persistenti e, pertanto, il processo di creazione dovrebbe supportare la collaborazione multi-strumento e multi-utente, nonché l'editing simultaneo durante l'esecuzione dal vivo.

Olitec ®© Laboratorio di Ricerca e Sviluppo presso
Fondazione Olitec Caritate Christi - olimaint©® is a trade mark of Olimaint Company
Brescia Via Saleri 55/58 - Italy (EU)
Valmontone via Colle S.Angelo 2/O - Italy (EU)

www.olimaint.tech - desk@oliverso.it

☏ +39 030 364332 int 5 +39 345 563 0496

Esperienze e mondi virtuali saranno assemblati da più tipi di dati e fonti di dati, comprese variazioni di tipi di dati 3D e media non 3D come audio, video ecc., oltre a tipi di media aggiuntivi ancora da prevedere.

Dato che siamo agli albori dello sviluppo del metaverso, la prossima generazione di Internet, è fondamentale che la standardizzazione non inibisca l'innovazione e la concorrenza e che sia orientata al soddisfacimento di alcuni principi di natura tecnico pratica :

- La rappresentazione di complesse scene statiche, ma anche mondi virtuali dinamici ed esperienze interattive compreso presentazione coerente (live-rendering) e rendering attraverso diversi strumenti.
- L'aggregazione di scene da oggetti rappresentati in una serie di formati, in particolare standard esistenti, inclusi oggetti 3D, audio, video e altri tipi di media.
- Caricamento, modifica e salvataggio di esperienze/scene, o parte di esse, contemporaneamente e in modo collaborativo utilizzando più strumenti di creazione mentre il contenuto è attivo, disponibile e condiviso (ovvero persistente).
- La definizione di elementi della scena come oggetti, geometria, materiali, luci, fisica, comportamenti in una forma che consente un semplice e senza perdita conversione tra formati ad esempio USD e glTF, o relativi sottoinsiemi.
- Sfruttare i meccanismi esistenti per estendere gli standard e i progetti open source per sperimentare meccanismi avanzati come sistemi procedurali di generazione di contenuti, rigging, logica, framework di interattività, streaming audio e video spaziale.
- Meccanismi di trasformazione dei dati che possono prendere risorse generalizzate e generare proceduralmente rappresentazioni specifiche della piattaforma e ottimizzate dell'esperienza/scena per prestazioni di runtime(1) ottimali su ciascuna piattaforma di destinazione.
    - (1) Esplorazione per consentire prestazioni di runtime ottimali di contenuto creato interoperabile in vari ambienti, comprese piattaforme commerciali native esistenti e standard 3D basati su browser come WebGL, WebGPU e WebAssembly. Ottimizzazione delle rappresentazioni dei contenuti 3D per soddisfare le capacità e i requisiti prestazionali di diverse piattaforme di runtime (ad esempio, supporto per geometrie ottimizzate o formati di texture, LOD ecc.) e identificare opportunità per creare risorse o tecniche condivise per automatizzare e facilitare questo processo.

Olitec ®© Laboratorio di Ricerca e Sviluppo presso
Fondazione Olitec Caritate Christi - olimaint©® is a trade mark of Olimaint Company
Brescia Via Saleri 55/58 - Italy (EU)
Valmontone via Colle S.Angelo 2/O - Italy (EU)

www.olimaint.tech - desk@oliverso.it

☏ +39 030 364332 int 5 +39 345 563 0496

Una tecnologia estensiva e le sue regole

La tecnologia che sta alla base delle applicazioni cosiddette di metaverso, un termine utilizzabile dal punto di vista commerciale e comunicativo ma che non indica alcun tipo di presupposto di natura tecnica, è una tecnologia che si basa su dei solidi principi che sono stati scritti ed istituiti a partire dagli anni 90 e che hanno visto la luce grazie all'intuizione di un gruppo di lavoro prevalentemente composto da sistemisti e sviluppatori italiani, tanto è vero che, a fatica, si sta affermando il diritto storico alla paternità del metaverso come prodotto dell'ingegno italiano.

La tecnologia ad oggi con le innumerevoli migliorie e con i protocolli scritti e migliorati è di per sé dal punto di vista infrastrutturale la base sulla quale la totalità delle applicazioni ad architettura distribuita, che sfrutteranno una trasmissione di informazioni a 100 terabit al secondo, che è stata a livello globale indicata quale nuova tipologia di struttura (6G) sulla quale la complessità della rete Internet andrà ad operare e sulla quale fra l'altro già stanno migrando la stragrande maggioranza delle piattaforme delle applicazioni oggi conosciute a livello internazionale e non solo, andranno ad operare.

Una capacità di coadiuvare l'essere umano e di ampliarne la sua potenzialità per effetto dell'inserimento di una serie di regole tecniche e protocolli che rimettono l'individuo al centro della tecnologia e non lo relegano più al mero ruolo di destinatario di un servizio o addirittura ancora peggio di prodotto venduto da un determinato servizio digitale.

Per questo ed è di fondamentale importanza le applicazioni che sfruttano la modalità immersiva e che la utilizzano appoggiandosi ad una architettura a carattere distribuito si stanno orientando sempre di più ad integrare protocolli di autenticazione che siano disgiunti da un erogatore intermedio quali ad esempio i fornitori di account per l'accesso all'utilizzo di servizi digitali, si veda la nota seguente descrittiva del protocollo HBA.

La parte innovativa prevalente relativa allo sfruttamento delle enormi potenzialità della realtà immersiva e dell'architettura distribuita e che si basa su 8 principi fondanti che ne regolamentano in maniera scientifica non solo le caratteristiche tecniche con le quali un'applicazione deve essere realizzata, ma soprattutto tendono a delineare un modello di programmazione e di distribuzione del dato che riprende i presupposti sopra citati ovvero la centralità dell'individuo e intorno ad esso la proprietà esclusiva del dato interno al soggetto utilizzatore.

Ad oggi non possiamo determinare quale forma assumerà nei prossimi 15 anni il metaverso con certezza, questo non è estremamente importante, quello che conta è che un giorno non molto lontano e quasi sicuramente entro l'anno 2030 assisteremo alla costruzione e all'implementazione funzionale di una rete globale di contenuti spazialmente organizzati, prevalentemente

Olitec ®© Laboratorio di Ricerca e Sviluppo presso
Fondazione Olitec Caritate Christi - olimaint©® is a trade mark of Olimaint Company
Brescia Via Saleri 55/58 - Italy (EU)
Valmontone via Colle S.Angelo 2/O - Italy (EU)

www.olimaint.tech - desk@oliverso.it

☏ +39 030 364332 int 5 +39 345 563 0496

tridimensionali, che saranno disponibili a chiunque senza alcun tipo di restrizione per l'uso in tutte le attività dell'essere umano : un mezzo nuovo e profondamente trasformativo, reso possibile da importanti innovazioni nell'hardware, nell'interfaccia uomo computer, nell'infrastruttura di rete e negli strumenti di creazione delle economie digitali.

E come accennavamo sopra esistono 8 regole, la prima regola o primo principio ci indica che il metaverso è unico non è frazionato non è frammentato, non è suddiviso in terreni, ed è la somma totale di tutti i mondi virtuali che sono accessibili al pubblico con i loro contenuti tridimensionali in tempo reale ed i relativi media collegati su di una rete globale e aperta non controllata da nessuno ed accessibile a tutti.

Questo primo principio ci deve portare a comprendere quale sia effettivamente la portata regolatoria per far sì che un'applicazione sia identificabile come applicazione meritevole di ottenere la qualifica di sistema predisposto per la realtà immersiva basato su architettura distribuita, ci permette anche di comprendere come sarà operativamente lo svolgimento dell'operatività digitale all'interno di questi mondi costruiti, mondi che nella realtà si tramutano in applicazioni software e che operano in maniera interoperabile tra di loro attraverso la condivisione di protocolli che sempre più stanno avvicinando la maggior parte degli sviluppatori mondiali in una uniformità di trasmissione delle informazioni e di capacità di movimentazione da un'applicazione all'altra senza necessariamente ricorrere alla pratica fastidiosa della accounting.

A seguire il principio numero due ci riporta indietro con la memoria a quasi cinquant'anni fa quando i padri fondatori del moderno Internet, i costruttori di ARPANET (Advanced Research Projects Agency Network), avevano sancito un desiderio attraverso il quale la rete nasceva per non avere limiti e barriere. Quando il secondo principio ci indica che il metaverso è per tutti fa riferimento alle nostre più ampie regole sociali di inclusione, questa non è chiaramente una dichiarazione di natura politica o socio economica ma è una constatazione di carattere etnografico che ha implicazioni politiche e socio economiche. Avere una struttura di distribuzione del dato basata sull'architettura di rete distribuita e renderla disponibile a chiunque proprio in funzione della tipicità e della particolarità della modalità di programmazione con le quali le applicazioni di metaverso vengono realizzate rende di fatto accessibile a chiunque con qualsiasi tipologia di device l'accesso ai contenuti ed alla possibilità di intraprendere relazioni digitali a 360 ° senza sopportare il peso del digital divide e senza sovrastare le regole di uguaglianza che sono sempre alla base della nascita di qualsiasi comunità digitale che basa il suo principio fondante, in questo caso identificato dal secondo principio, sul fatto che tutti debbano avere uguale accesso all'informazione e alla rete e sul fatto che tutti debbano poter trasferire informazione e riceverne altrettanta in maniera libera e indipendente.

E viene da se che questo ci porta all'introduzione del terzo principio quello che determina come non debba esistere un controllore del metaverso, questo perché esso è un bene comune universale per la comunicazione digitale e il commercio, può essere intermediato secondo specifiche necessità e

Olitec ®© Laboratorio di Ricerca e Sviluppo presso
Fondazione Olitec Caritate Christi - olimaint©® is a trade mark of Olimaint Company
Brescia Via Saleri 55/58 - Italy (EU)
Valmontone via Colle S.Angelo 2/O - Italy (EU)

www.olimaint.tech - desk@oliverso.it

☏ +39 030 364332 int 5 +39 345 563 0496

che rispettano le leggi istitutive, è governato come richiesto dall'interesse comune verso il massimo bene per il maggior numero di persone; la mancanza di controllo nel metaverso non deve essere confusa con una struttura informatica e sistemistica traballante e pericolosa, tutt'altro, non viene indicato una mancanza di controllo nell'elaborazione dell'informazione ma viene fortemente iscritto il principio per il quale nessun soggetto sia esso pubblico o privato può detenere un controllo sulle applicazioni che compongono il metaverso e sui soggetti che lo popolano, oggi nel mondo dell'architettura centralizzata e decentralizzata assistiamo esattamente al contrario dove siamo necessariamente sottoposti al controllo di soggetti terzi che dominano da posizioni prevalenti di mercato e impongono la loro linea operativa e di pensiero in modo trasversale in tutti e cinque i continenti e in tutti i paesi del mondo, la necessità per i padri costituenti di indicare e di vietare di assumere il controllo di tutto il metaverso completo e di per sé la risposta assonante uguale contraria dove quando non c'è un unico controllore del metaverso di fatto democraticamente è la completa rete che controlla se stessa e quindi rimanda il principio alla centralità dell'essere umano come soggetto intorno al quale la struttura viene plasmata e implementata anche nel progresso tecnologico che periodicamente sta facendo balzi da gigante in avanti. Questo principio non è discutibile anche se è l'oggetto di numerosi conflitti di natura tecnico scientifica all'interno dei gruppi di ricerca e di studio perché il governo e il controllo di un ecosistema così complesso come quello del metaverso, che rispetto alle infrastrutture attuali contiene una serie di ulteriori e preziosissime serie di dati, non può essere relegato nelle mani di alcuno fosse anche di più persone se non di tutte le persone che concorrono alla costruzione della rete.

E per logica ci si riporta alla scrittura del quarto principio dove viene chiaramente indicato che il metaverso è un sistema aperto, che si basa su tecnologie e strumenti interoperabili collegati tramite standard di comunicazione liberi e aperti e rigorosamente definiti e ampiamente concordati; questo aspetto è essenziale per quanto riguarda la possibilità della libera circolazione delle idee e delle informazioni e della parola e non prevede, proprio perché è governato dai tre principi precedenti alcun tipo di imposizione seppur anche di tipo etico e giurisdizionale.

L'interoperabilità è la vera sfida dell'eccellenza di questa tecnologia rispetto alle precedenti che sono state fallimentari nel proporre dei modelli liberi ma liberi con un contingentamento di mobilità da parte dell'utente stesso che si è trovato necessariamente obbligato ad accettare suo malgrado una serie di imposizioni e forzature digitali che spesso hanno anche travalicato le norme dei paesi sovrani. L'interoperabilità è quella caratteristica essenziale che ci permette di poter passare da un ambiente all'altro in maniera libera e rapida senza la necessità di essere obbligatoriamente condizionati dall'apertura e dal trasferimento di dati e informazioni all'interno di molte piattaforme che coesistono sulla stessa rete ma che di fatto vivono un ecosistema proprietario chiuso e vincolato, l'utente ha necessità di potersi muovere liberamente all'interno dell'ecosistema del metaverso e la sua apertura, ovvero l'interoperabilità, è la struttura essenziale che porterà realmente questa architettura e questa tecnologia ad essere quella che ci accompagnerà per i prossimi 30 anni della nostra storia su questo pianeta.

Olitec ®© Laboratorio di Ricerca e Sviluppo presso
Fondazione Olitec Caritate Christi - olimaint©® is a trade mark of Olimaint Company
Brescia Via Saleri 55/58 - Italy (EU)
Valmontone via Colle S.Angelo 2/O - Italy (EU)

www.olimaint.tech - desk@oliverso.it

☏ +39 030 364332 int 5 +39 345 563 0496

Trattiamo sempre di parlare di metaverso dal punto di vista del software ma questa tecnologia ha anche una enorme componente che guarda alla parte hardware, ovvero, a quella parte di strutture integrate che permettono la fruizione dei contenuti dei software di realtà immersiva e architettura distribuita realizzati. Qui nasce l'esigenza di normare un aspetto fondamentale che è quello della indipendenza dall'hardware ovvero della accessibilità su qualsiasi dispositivo indipendentemente dal tipo di visualizzazione o dal fattore di forma e soprattutto una accessibilità pari e/o superiore per le persone disabili rispetto alle persone normodotate.

L'applicabilità del quinto principio di fatto sancisce anche l'interruzione ed una vittoria socioeconomica sull'annoso problema del digital divide che grazie proprio alla normalizzazione, e quindi alla obbligatorietà di scrivere applicazioni che possano funzionare su qualsiasi dispositivo al quale l'utente può accedere, può permettere la vera esecuzione del secondo principio ovvero che il metaverso è per tutti e diventa una constatazione di carattere etnografico con implicazioni politiche e socio economiche.

Abbiamo parlato di applicazioni e di hardware e quindi dobbiamo sicuramente entrare adesso nel merito della valutazione di ciò che permette a tutti questi sistemi di poter coesistere ovvero la rete, di fatto la nascita è il ragionamento che sta alla base del sesto principio è che il metaverso è una rete di computer che collega le esperienze virtuali pubblicamente accessibili, i suoi contenuti tridimensionali e i suoi media, e la cui novità rispetto alle reti del passato è che presenta le informazioni digitali nella forma di spazi, posti, oggetti e utenti tridimensionali, questo facilita estremamente la comunicazione soprattutto perché utilizza ambienti che sono persistenti da una sessione all'altra cioè le modifiche applicate tanto quanto nella realtà restano anche nelle applicazioni di metaverso e il fatto che il metaverso sia una rete di computer e che sfrutti il principio dell'architettura di rete distribuita ci porta anche ad analizzarne quelli che sono i vantaggi sostanziali e del perché l'applicazione che rispetta gli 8 principi viene definita in termini tecnici, con anche un po' di affetto e romanticismo, highlander application ovvero applicazione immortale in quanto si desume che la funzionalità di un'applicazione che rispetta gli 8 principi, scritta per far sì che essi vengano completamente rispettati, ha la sua funzionalità fino al momento in cui sul pianeta almeno due computer saranno interconnessi tra di loro.

Questo ci fa capire quanto le tre anime che costituiscono la parte di metaverso siano necessariamente e obbligatoriamente inscindibili l'una all'altra questo perché non può esistere metaverso senza rete, come non può esistere rete senza device, come non possono esistere device senza software che permettono la trasmissione di dati sulla rete.

Olitec ®© Laboratorio di Ricerca e Sviluppo presso
Fondazione Olitec Caritate Christi - olimaint©® is a trade mark of Olimaint Company
Brescia Via Saleri 55/58 - Italy (EU)
Valmontone via Colle S.Angelo 2/O - Italy (EU)

www.olimaint.tech - desk@oliverso.it

☏ +39 030 364332 int 5 +39 345 563 0496

E per deduzione e logica ci portiamo al settimo principio e viene da sé che la definizione più naturale che può nascere da noi è che il metaverso niente altro è che Internet, migliorato ed aggiornato per fornire costantemente dei contenuti di natura immersiva delle informazioni e delle esperienze organizzate nello spazio con una comunicazione sincrona in tempo reale.
Ci arrabattiamo a trovare spiegazioni a ciò che nella realtà abbiamo davanti sostanzialmente da tutta una vita, le applicazioni di realtà immersive di metaverso vedono la luce a partire dagli anni 90 e hanno accompagnato tutto questo percorso tecnologico e sono arrivate fino ai giorni nostri quasi in maniera silenziosa e rispettosa del progresso che altre tecnologie, molto meno performanti ed umanizzanti, stavano ottenendo prevalentemente orientate dalla parte commerciale e di controllo umano; basti pensare alla storia, al funzionamento, e agli obiettivi di tutte le odierne moderne applicazioni di social network.

Per molti anni queste sono state le leggi che hanno retto lo sviluppo di applicazioni di metaverso, questo significa che lo sviluppatore per essere coerente e per poter produrre un'applicazione reale e vera di metaverso deve far sì che la stessa applicazione rispetti completamente tutte le regole precedentemente scritte, questo però non presuppone che non possano essere aggiornate o di integrate ed è per questo che nel 2021 si è valutato, vedendo una crescita esponenziale delle attività legate alle criptovalute, che troppo spesso sfociavano in applicazioni non propriamente corrette e lecite, di chiarire in maniera molto marcata che esisteva una differenza sostanziale tra il metaverso e il mondo delle criptovalute e anche della blockchain e allora si è andati a definire l'ottavo principio che quindi completa la gamma dei principi sui quali le applicazioni di metaverso devono essere costruite.

L'ottavo principio ci dice che la valutazione sulla libertà di azione deve essere anche intesa come libertà economica quindi se l'utente che vuole utilizzare delle applicazioni di metaverso e non vuole acquisire obbligatoriamente una valuta forzata deve essere libero di farlo, se vuole utilizzare delle valute riconosciute dalla comunità è libero di farlo quindi da questo punto di vista ribadiamo forte che il concetto di metaverso equivale al concetto di libertà e qualsiasi azione che va a contrastare con una delle 8 leggi, anche solo una delle 8 leggi ne vanifica l'esperienza e non permette concettualmente di identificare come metaverso l'applicazione nella quale stiamo in questo momento operando.

Cosa significa questo ? Significa che abbiamo in un principio due principi : il primo che il metaverso è svincolato da qualsiasi valuta sia essa digitale o ordinaria e questo significa che operativamente noi possiamo sviluppare applicazioni di metaverso che trattano l'uso di valuta, che trattano l'uso di criptovaluta o che non trattano né una né l'altra in maniera libera e quindi rispettosa dei principi precedenti e non vincolante per l'utente, ovvero non deve essere un requisito vincolante la trattazione di una valuta o peggio ancora l'acquisizione forzata di una valuta per poter accedere all'applicazione di metaverso e il secondo principio che sta all'interno dell'ottavo principio è quello

Olitec ®© Laboratorio di Ricerca e Sviluppo presso
Fondazione Olitec Caritate Christi - olimaint©® is a trade mark of Olimaint Company
Brescia Via Saleri 55/58 - Italy (EU)
Valmontone via Colle S.Angelo 2/O - Italy (EU)

www.olimaint.tech - desk@oliverso.it

☏ +39 030 364332 int 5 +39 345 563 0496

che ci dice banalmente, che quindi va a chiudere completamente in maniera ermetica il cerchio, che nel caso in cui un'applicazione sviluppata per il metaverso non rispetti tutti e gli 8 i principi che abbiamo enunciato fino ad adesso questa applicazione non sarà un'applicazione costruita per il metaverso, sarà un'applicazione sicuramente eccezionale un'applicazione tridimensionale un'applicazione basata su criptovalute ma non sarà un'applicazione che a livello internazionale verrà riconosciuta come applicazione di metaverso e quindi meritevole di ottenerne tutti i benefici che ne conseguono.

Olitec ®© Laboratorio di Ricerca e Sviluppo presso
Fondazione Olitec Caritate Christi - olimaint©® is a trade mark of Olimaint Company
Brescia Via Saleri 55/58 - Italy (EU)
Valmontone via Colle S.Angelo 2/O - Italy (EU)

www.olimaint.tech - desk@oliverso.it

☏ +39 030 364332 int 5 +39 345 563 0496

Scheda tecnica di analisi, modalità di valutazione

Per poter verificare se un'applicazione rientra tra quanto sopra sommariamente brevemente indicato si può utilizzare una griglia di controllo che deve andare a verificare necessariamente la presenza di tutti i punti che sono indicati al suo interno, la sola mancanza di uno di questi requisiti fa decadere la classificazione dell'applicazione come applicazione di metaverso.

La tabella successiva indica parametro per parametro la descrizione specifica di cosa deve essere valutato per l'analisi dell'attribuzione di una valorizzazione e quindi dell'assegnazione di un contributo finanziario relativamente ad un'applicazione di meta verso, la base totale del punteggio attribuito per importanza di parametro è pari a 100, il range di accettabilità dell'applicazione si può basare in una valorizzazione che stia tra 90 e 100 pti e che abbia al suo interno il rispetto, anche in base ponderale con un punteggio inferiore, ma di tutti i punti descritti nessuno escluso.

Parametro	Descrizione Parametro	Pti	Note
Requisiti architetturali	Vanno analizzati quelli che sono i requisiti strutturali dell'applicazione, in particolar modo per prima cosa va verificato se realmente la struttura dell'applicazione è creata all'interno di un architettura distribuita che è un elemento essenziale per far sì che l'applicazione rientrano nella categorizzazione delle tipologie di software che comunemente chiamiamo metaversi.	10	
Matrice di sviluppo	Bisogna verificare con quale tool di sviluppo l'applicazione è stata realizzata, in base a questo è possibile comprendere se la finalità dell'applicazione è quella della creazione di un metaverso che rispetta gli otto principi oppure se risulta essere solamente un mondo tridimensionale senza le prerogative tipiche degli elementi fondativi delle applicazioni immersive.	5	
Interoperabilità	Va verificata la interoperabilità dell'applicazione con altre applicazioni analoghe, e la capacità di acquisire la programmazione Avatar che non necessiti obbligatoriamente di una procedura di accounting informatico e che quindi richieda l'utente l'utilizzo di diversi accessi in funzione delle diverse applicazioni che deve utilizzare, per esemplificare la creazione di un avatar, ovvero l'account attraverso il quale l'utente accede all'applicazione di metaverso e si muove con esso al suo interno, deve essere costruito attraverso delle applicazioni che rispecchiano e rispettano le regole costitutive del metaverso e che sono interoperabili ovvero la creazione dell'avatar attraverso tutti questa natura permette all'utente con lo stesso Avatar di poter navigare su mondi differenti, questo è un requisito fondamentale perché significa che l'applicazione è stata strutturata per essere basata sui principi fondanti e sulle tecniche di programmazione standardizzate ed interoperabili che sono alla base delle reali applicazioni di metaverso.	10	

Olitec ®© Laboratorio di Ricerca e Sviluppo presso
Fondazione Olitec Caritate Christi - olimaint©® is a trade mark of Olimaint Company
Brescia Via Saleri 55/58 - Italy (EU)
Valmontone via Colle S.Angelo 2/O - Italy (EU)

www.olimaint.tech - desk@oliverso.it

☏ +39 030 364332 int 5 +39 345 563 0496

Rispetto del 5° principio	Bisogna attestare la funzionalità dell'applicazione a livello di device trasversale, l'applicazione deve essere in grado di funzionare in maniera simultanea e condivisa su tutte le tipologie di device oggi esistenti sul mercato, qualora questo non avvenisse l'applicazione non si può ritenere un'applicazione di metaverso ma una semplice banale applicazione tridimensionale.	10	
Accessibilità	Verificare la condivisione dell'ambiente che deve essere fruibile da più soggetti contemporaneamente generando la rappresentazione effettiva e reale della condivisione di risorse, per esemplificare, un ambiente che rientra nella tipologia tecnica delle applicazioni di metaverso deve permettere ad un numero di Avatar di essere contestualmente contemporaneamente presenti all'interno dello stesso ambiente e di poter fruire di una serie di servizi tecnici.	8	
Comunicazione	Avere l'accesso a sistemi audio e video e a sistemi di sostituzione delle vecchie piattaforme di videoconferenza sostituite da sistemi di dialogo interno all'ambiente sviluppato.	5	
Compatibilità iot e opm	Essere compatibili con i protocolli opm e quindi per mettere anche l'integrazione e la capacità di inviare da acquisire comandi e informazioni all'interno e all'esterno dell'applicazione	9	
Standard di progettazione	Basare lo sviluppo degli oggetti tridimensionali inseriti in prevalenza sulla programmazione di oggetti con estensione glb e glft o fbx convertibili come stabilito dalla nota MSF 2022 sulla standardizzazione degli elementi.	10	
BIM	Permettere l'integrazione e le esportazione di oggetti che rientrano nelle categorie bim[(2)]	5	(2) Il Building Information Modeling indica un metodo per l'ottimizzazione della pianificazione, realizzazione e gestione di costruzioni tramite aiuto di un software. Tramite esso tutti i dati rilevanti di una costruzione possono essere raccolti, combinati e collegati digitalmente.
Traduzione	Avere a disposizione un algoritmo di traduzione simultanea che permetta di poter fare interagire i soggetti all'interno dell'ambiente in maniera naturale e fluida anche nella conversazione diretta.	3	
Controllo diritti	Avere un ambiente che sia dotato di protocolli di verifica del rispetto del diritto d'autore tipo OPM VK1 o similare.	7	
Attestazione	L'applicazione di metaverso per essere tale deve essere preferibilmente censita e registrata all'interno del registro t42 o in alternativa presso i registri comunitari euipo o internazionali wipo rispettando le dinamiche del protocollo di Lisbona	4	
Sviluppatore	Gli sviluppatori che realizzano l'applicazione di metaverso o di architettura distribuita per realtà immersiva devono preferibilmente aver conseguito un titolo di abilitazione o	4	

Olitec ®© Laboratorio di Ricerca e Sviluppo presso
Fondazione Olitec Caritate Christi - olimaint©® is a trade mark of Olimaint Company
Brescia Via Saleri 55/58 - Italy (EU)
Valmontone via Colle S.Angelo 2/O - Italy (EU)

www.olimaint.tech - desk@oliverso.it

☏ +39 030 364332 int 5 +39 345 563 0496

	certificazione VRO da ae01 ad ae04 (possibilmente riscontrabili nei registri di abilitazione consultabili on line).		
Valorizzazione	La valorizzazione dell'applicazione deve basarsi su parametri univoci, come per esempio l'mmq o m^2 equivalente e non superare quelli che sono i parametri generali stabiliti a livello di convenzioni internazionali nella valorizzazione per unità di misura.(3) (3) in questo specifico contesto possiamo anche sbilanciarci nel definire quello che potrebbe essere un valore massimo di realizzazione di un'applicazione di metaverso basata sul parametro del metro quadro equivalente, ovvero dello spazio che nella realtà viene occupato dall'applicazione è riferito ad un ipotetico spazio reale, ad oggi la media internazionale sulla valorizzazione dell'MMQ e di 50 $ per singola unità si deve però badare bene a questo aspetto che il valore non indica solamente il costo di produzione e realizzazione dell'applicazione ma anche integra l'obbligatorietà del mantenimento a vita del prodotto e comunque per un periodo non inferiore a 5 anni	7	(3) in questo specifico contesto possiamo anche sbilanciarci nel definire quello che potrebbe essere un valore massimo di realizzazione di un'applicazione di metaverso basata sul parametro del metro quadro equivalente, ovvero dello spazio che nella realtà viene occupato dall'applicazione è riferito ad un ipotetico spazio reale, ad oggi la media internazionale sulla valorizzazione dell'MMQ e di 50 $ per singola unità si deve però badare bene a questo aspetto che il valore non indica solamente il costo di produzione e realizzazione dell'applicazione ma anche integra l'obbligatorietà del mantenimento a vita del prodotto e comunque per un periodo non inferiore a 5 anni
Persistenza	La persistenza delle modifiche effettuate in tempo reale, in ottica di autosaving è fondamentale in un'applicazione VRO in quanto ogni soggetto, che ne ha il permesso, deve essere in grado di ritrovare la condizione dell'applicazione come il momento ultimo nella quale l'ha lasciata e stessa cosa vale per ogni soggetto che popola il metaverso	3	

Olitec ®© Laboratorio di Ricerca e Sviluppo presso
Fondazione Olitec Caritate Christi - olimaint©® is a trade mark of Olimaint Company
Brescia Via Saleri 55/58 - Italy (EU)
Valmontone via Colle S.Angelo 2/O - Italy (EU)

www.olimaint.tech - desk@oliverso.it

☏ +39 030 364332 int 5 +39 345 563 0496

Attività ammissibili che possono utilizzare la tecnologia VRO Nota di attualità esemplificativa non vincolante

Manifestazioni Fieristiche e B2B in tecnologia VRO Metaverso

Le fiere VRO sono applicazioni sviluppate con tecnologia VRO che permettono la realizzazione e la rappresentazione di una fiera reale in tutto e per tutto.

In un'ottica globale dove sempre di più stiamo vedendo il verificarsi di contrazioni a livello della capacità di investimento in trasporti e soprattutto per quanto concerne il comparto energetico, l'intuizione del laboratorio di ricerca Olitec è stata di anticipare i tempi e quindi di iniziare a presentare al mercato degli espositori abituali nonché degli organizzatori di eventi, loro associati, un gemello digitale in tutto e per tutto fedele all'originale che permettesse di offrire contestualmente agli operatori una postazione fisica e la gemella postazione digitalizzata; una vision salvagente anche per scenari futuri ma soprattutto una vision che permette e permetterà di mantenere aperte tutte quante le fiere che normalmente hanno una durata limite nel tempo per tutta la durata dell'anno sfruttando tutte le tecnologie della VRO e le funzionalità delle cosiddette "SubVRO" ovvero degli enviroment gemellati che possono riprodursi pressoché all'infinito mantenendo la costanza dell'applicazione iniziale e non gravando sulle risorse del sistema informatico della sua architettura.

La conformazione di ogni singolo progetto di plesso espositivo è strutturata nella operatività reale del plesso fieristico ed è organizzata riproducendo completamente tutti i padiglioni fieristici nelle misure reali per una superficie totale complessiva, per singolo enviroment, superiore ai 200.000 metri quadrati, all'interno inoltre sono stati realizzati alcuni ambienti in uso comune quali l'Auditorium centrale posto nel lato nord ovest del complesso espositivo che ha capacità di contenere fino a 500 persone contemporaneamente con la traduzione simultanea in 14 lingue.

All'interno i singoli padiglioni possono ospitare una o più manifestazioni contemporaneamente o attività o eventi di altro tipo e sono completamente indipendenti l'uno all'altro, quindi la struttura può far condividere diverse esperienze a diversi soggetti inter connettibili tra di loro semplicemente passando da un padiglione all'altro.

La struttura come abbiamo detto si compone di molti più plessi operativi che riproducono fedelmente quelli della realtà espositiva, ed è proprio questa volontà di realizzare un ambiente completamente simile all'ambiente dove il visitatore può vivere la sua esperienza reale che ha entusiasmato i primi organizzatori storici di eventi all'interno dei plessi digitali, ragionando di strutturare in questo momento le loro manifestazioni utilizzando sia il canale tradizionale espositivo fisico sia in parallelo il canale espositivo digitale anche in previsione di quelle che potrebbero essere delle future

Olitec ®© Laboratorio di Ricerca e Sviluppo presso
Fondazione Olitec Caritate Christi - olimaint©® is a trade mark of Olimaint Company
Brescia Via Saleri 55/58 - Italy (EU)
Valmontone via Colle S.Angelo 2/O - Italy (EU)

www.olimaint.tech - desk@oliverso.it

☏ +39 030 364332 int 5 +39 345 563 0496

contrazioni a livello mondiale nei trasporti e nei movimenti di merci e di persone dovute alla sempre crescente crisi globale energetica.

La struttura opererà attraverso un architettura decentralizzata di secondo livello che sostanzialmente permette una velocità e un'interazione molto più rapida rispetto ai processi operativi analoghi del passato e gli espositori avranno la facoltà di costruire di personalizzare e di gestire i propri stand proprio nello stesso identico modo con il quale lo fanno nell'esposizione reale, ovvero in maniera diretta oppure incaricando degli operatori digitali abilitati affinché possano strutturare e realizzare il loro stand che sarà costruito secondo le prerogative di ogni singolo espositore. Proprio per questo saranno fruibili periodicamente dei corsi live gratuiti per insegnare agli operatori a personalizzare gli stand.

E nello stand si potrà incontrare un operatore reale che attraverso il collegamento tramite un device, magari comodamente seduto in azienda, potrà intrattenere i visitatori accompagnandoli nella loro visita e presentando loro le opportunità che i prodotti e servizi dell'azienda rappresentata può offrire loro, e si può arrivare ad ottenere un risultato veramente performante perché l'iterazione che si ha non è l'iterazione che si può avere tra un uomo e una macchina come per esempio nella verifica e nell'utilizzo di sistemi basati su architetture web tradizionali ma è un'interazione che si ottiene attraverso un altro individuo che, seppur collegato in remoto, è reale e risponde in tempo reale agli stimoli umani che riceve e permette di offrire e dimostrare tutto ciò che avrebbe potuto fare nella realtà però attraverso la rappresentazione tridimensionali immersive.

Prende sempre più corpo quindi la capacità di poter trasferire l'esperienza reale di tipo espositivo in un'esperienza reale di tipo "espositivo digitale" finalizzata all'avvicinamento di un numero sempre maggiore di visitatori e di utenti interessati e soprattutto senza quella freddezza che i sistemi tradizionali di tecnologia web 2 ci hanno abituato ad avere quando parliamo di applicazioni che impiegano contemporaneamente più tecnologie.

Ma non parliamo di applicazioni all'interno delle quali si fanno delle interrogazioni a diversi tipi di database ma parliamo di applicazioni all'interno delle quali il soggetto che andiamo a interrogare non è un database che risponde in maniera fredda semplicemente alla nostra ricerca ma è un individuo che è collegato dall'altra parte con tutte le peculiarità le prerogative dell'individuo stesso.

Per questo le applicazioni che vengono sviluppate con la metodologia e con la tecnologia integrata VRO risultano essere molto più accettate e molto più utilizzabili da qualsiasi tipologia di utente di qualsiasi fascia di età e di estrazione sociale e soprattutto di qualsiasi tipologia di conoscenza tecnica e tecnologica, non serve quindi essere degli esperti informatici per poter passeggiare all'interno di una fiera digitale costruita in VRO.

Olitec ®© Laboratorio di Ricerca e Sviluppo presso
Fondazione Olitec Caritate Christi - olimaint©® is a trade mark of Olimaint Company
Brescia Via Saleri 55/58 - Italy (EU)
Valmontone via Colle S.Angelo 2/O - Italy (EU)

www.olimaint.tech - desk@oliverso.it

☏ +39 030 364332 int 5 +39 345 563 0496

Nascono quindi anche dei posizionamenti cosiddetti **KioskVro** ovvero delle postazioni dotate di tecnologia OPM(r)(c) e OLD(r)(c) proprietario di olimaint che sono in grado di offrire all'utente l'accesso immediato alla room **semplicemente sedendosi davanti al monitor** collegato con la telecamera senza necessità di dover digitare alcunché e senza necessità di dover fare alcun tipo di operazione informatica.

È sicuramente estremamente interessante la possibilità della gestione diretta dello stand modificabile just in time e in ogni momento del giorno per poterlo aggiornare con le novità che l'espositore ritiene di dover presentare al mercato.

La fiera sarà fra l'altro la prima dotata di **Avatar Hostess** digitali che si muoveranno lungo tutte le superficie del plesso espositivo fornendo consigli su quali stand digitali visitare e distribuendo dei depliant sempre digitali che verranno consegnati da Avatar ad Avatar e che l'utente si troverà scaricati automaticamente o all'interno della propria mail come allegato o nel download automatico che la VRO, ovviamente con il consenso, trasferirà archiviandoli nella memoria del suo device.

Si apre quindi un percorso nuovo entusiasmante che permetterà sia ai detentori dei plessi espositivi ma soprattutto agli organizzatori di eventi di poter sviluppare un nuovo modello di fiera perdurante nel tempo e continuamente aggiornata aumentando di gran lunga la fidelizzazione del cliente finale e del suo visitatore.

All'interno delle fiere VRO è possibile

- Acquisire uno stand standard o customizzato
- Personalizzare il proprio stand con loghi, oggetti 3D, immagini e video
- Organizzare eventi all'interno del proprio stand o all'interno degli auditorium
- Dialogare in 14 lingue senza la necessità di avere traduttori
- Vendere i propri prodotti e servizi attraverso il proprio portale online o tramite token
- Ricevere visitatori in ogni momento dell'anno e non solo nei giorni della fiera
- Beneficiare del flusso degli iscritti nei giorni di apertura della singola fiera
- Permettere di passare dal proprio stand immersivo nella fiera VRO alla propria VRO personale che magari riproduce l'azienda espositrice all'interno del quale ci sono tutte le produzioni, anche quelle oltre a ciò esposto in fiera
- Modificare in ogni momento l'allestimento dello stand
- Poter incontrare clienti e fornitori da ogni paese del mondo
- Avere una fiera che rimane costantemente aperte ed attiva
    - Poter realizzare dei gemelli digitali praticamente senza limite per avviare altre fiere nel web3
- Inviare e ricevere documentazione semplicemente passando negli stand
- Promuovere anche eventi a pagamento

Olitec ®© Laboratorio di Ricerca e Sviluppo presso
Fondazione Olitec Caritate Christi - olimaint©® is a trade mark of Olimaint Company
Brescia Via Saleri 55/58 - Italy (EU)
Valmontone via Colle S.Angelo 2/O - Italy (EU)

www.olimaint.tech - desk@oliverso.it

☏ +39 030 364332 int 5 +39 345 563 0496

Protocollo univoco di autenticazione dell'utente basato sul principio della interoperabilità

HUMAN BIOMETRIC AVATAR

L'avatar biometrico è un protocollo che permette l'autenticazione dell'individuo in maniera certa ed univoca nell'accesso ad altre applicazioni sviluppate nella tecnologia Web 3.

Per costruire un avatar biometrico abbiamo necessità di acquisire determinate informazioni effettivamente di natura personale dell'individuo che rendono, incrociate tra di loro, certa l'identità del soggetto che ne è effettivamente proprietario. in questo caso l'avatar biometrico quando si presenta alla porta di una applicazione fornisce il risultato di una elaborazione di tutti i dati acquisiti e ne verifica il corretto match con il soggetto reale in quel preciso momento.

i dati che vengono inseriti all'interno dell'avatar biometrico sono:

- impronte digitali (tutte)
- frequenza del battito cardiaco
- mappatura dell'iride (entrambe)
- mappatura del padiglione auricolare (entrambe)
- mappatura completa del genoma (quattro eliche)
- timbro vocale

L'algoritmo una volta che ha acquisito tutte queste informazioni è in grado di controllarle e verificarle attraverso un'acquisizione campionata ed incrociata delle stesse e utilizza determinati parametri biometrici solo in funzione di determinate applicazioni.

Questo significa che per esempio l'incrocio della mappatura completa del genoma non verrà utilizzato dal protocollo dell' Avatar per accedere alla consultazione di una banca dati ma verrà utilizzato in specifiche applicazioni sanitarie o di altra natura che richiedono un'analisi anche di quel tipo di informazione; questo da una parte per non disperdere risorse ed energie di elaborazioni inutili e dall'altra parte perché rende più rapido anche l'utilizzo del protocollo per accedere ad applicazioni che non richiedono una grande quantità di analisi sulle informazioni che compongono il set di dati dell'avatar.

Quindi quando noi vorremmo accedere ad un'applicazione nel metaverso che chiede la nostra autenticazione non dovremmo fare altro che presentarci alla porta dell'applicazione e mostrare le nostre credenziali senza però rilasciare alcun tipo di dato, alcun tipo di informazione che ci riguarda all'interno dell'applicazione.

Olitec ®© Laboratorio di Ricerca e Sviluppo presso
Fondazione Olitec Caritate Christi - olimaint©® is a trade mark of Olimaint Company
Brescia Via Saleri 55/58 - Italy (EU)
Valmontone via Colle S.Angelo 2/O - Italy (EU)

www.olimaint.tech - desk@oliverso.it

☏ +39 030 364332 int 5 +39 345 563 0496

Questa è una novità importante nell'ambito della gestione del dato personale che permette una serie di vantaggi non indifferenti come per esempio **l'impossibilità che qualcuno rubi le nostre credenziali** oppure **l'impossibilità di creare dei profili fasulli** questo perché è fisicamente impossibile duplicare un individuo con le medesime caratteristiche e soprattutto perché l'apertura e l'acquisizione di quei dati una volta che viene fatta nella creazione dell'avatar biometrico non può essere aperta e consultata da nessuno se non dal soggetto originario che ha costruito la BlockChain sulla quale sono appoggiati i riferimenti ai dati relativi ai parametri biometrici acquisiti.

Come le applicazioni del Web 3 e le amministrazioni pubbliche possono verificare il protocollo dell'avatar biometrico?

Attraverso delle telecamere dotate di sensori che già oggi sono in commercio, per quanto riguarda le applicazioni che richiedono anche l'analisi della mappatura genomica attraverso l'utilizzo di specifici analizzatori, software, che possono analizzare l'informazione genomica contenuta nell'avatar.

Quali potrebbero essere delle applicazioni pratiche nella vita di tutti i giorni dell'avatar biometrico?

Eccone alcune

- accesso sicuro a tutte le piattaforme Web 3 del mondo senza dispersione di dati personali
- verifica della compatibilità a determinate tipologie di farmaco senza l'obbligatorietà di effettuare dei test fisici
- autenticazione per operazioni e transazioni finanziarie
- autenticazione per attività nei confronti della pubblica amministrazione
- partecipazione ad atti notarili(*cosa questa peraltro già in via di sperimentazione e descritta nella massima numero 200 del collegio notarile di Milano*)
- sottoscrizione di contratti digitali
- partecipazione ad attività forensi
- sostituzione di tutte le procedure di autenticazione che oggi sono eseguite attraverso sistemi quali spid carta d'identità elettronica e posta elettronica certificata
- telemedicina evoluta
- accesso al proprio autoveicolo e messa in moto
- accesso alla propria abitazione a tutti i sistemi di domotica
- gestione di Smart TV e apparecchiature connesse
- verifica e compatibilità alimentare
- verifica e compatibilità farmacologica
- analisi e verifica della compatibilità genetica con terzi
- garanzia totale nell'impossibilità di clonazione delle credenziali in quanto non esistenti
- consegna e ritiro dei propri dati ad applicazioni terze solo per il tempo strettamente necessario ad elaborare le informazioni per nostro conto

Olitec ®© Laboratorio di Ricerca e Sviluppo presso
Fondazione Olitec Caritate Christi - olimaint©® is a trade mark of Olimaint Company
Brescia Via Saleri 55/58 - Italy (EU)
Valmontone via Colle S.Angelo 2/O - Italy (EU)

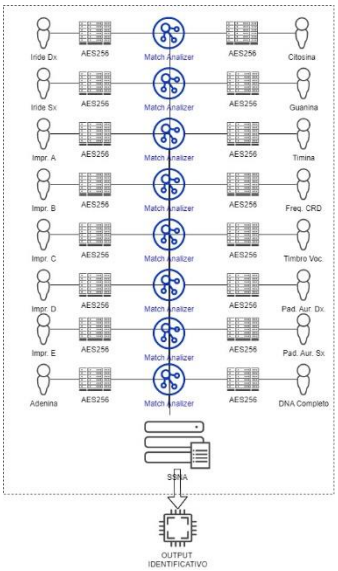
www.olimaint.tech - desk@oliverso.it

☏ +39 030 364332 int 5 +39 345 563 0496

- utilizzo di qualsiasi applicazione di metaverso esistente senza account
- ….e molto molto altro

L'avatar HBA è una tecnologia rivoluzionaria, un sistema di identificazione univoca che si basa su parametri di unicità dell'individuo, è alla base della nuova era dell'identificazione personale nel web3, basta spid, password, pec e altri sistemi di accreditamente basati su servizi di terzi, il vero account siamo noi ! Siamo unici come esseri umani e come tali siamo unici nella nostra unicità di esseri umani. L'acquisizione di quei dati una volta che viene fatta nella creazione dell'avatar biometrico non può essere aperta e consultata da nessuno se non dal titolare dei dati. Questi potrà condividerli autorizzandoli dimostrabilmente a chi vorrà e per il tempo che riterrà necessario. Normalmente condividerà solo un digest crittografico comprensivo della sua firma digitale che verrà confrontato con quello generato da chi dovrà autorizzarlo ad accedera a qualsiasi servizio. Tutti i suoi dati sono memorizzati in supporti protetti da accessi indesiderati e da cancellazioni su strutture distribuite altamente resilienti. Questi dati hanno una corrispondenza univoca con una scrittura in Blockchain Decentralizzate, Distribuite, public e permissionless.

Schemi funzionali HBA



L'HBA contiene 16 parametri che identificano dei indicatori biometrici individuali, ogni parametro viene caricato attriverso un protocollo DPS DBX che è preceduto in accesso da un chiave crittografata a 256 bit AES. Per caricare e modificare il dato è necessario possedere tutte le 16 chiavi di accesso una per ogni singolo parametro, come anche per modificarlo, inoltre le chiavi forniscono accesso ad un parametro singolo e non al completo set di parametri; quindi per accedere all SSNA (Sistema Scatola Nera di Autenticazione) tutti i Match Analizer, posti su ogni singolo nodo che interseca la rete di collegamento dei parametri tra di loro (ovvero 16^{16} connessioni) devono dare il GL (Green Light) previsto per far si che il SSNA consegni un output di conferma del soggetto identificato all'applicazione W3 che ne richiede la presentazione. Il protocollo HBA permette inoltre di
poter accedere all'SSNA anche con 12/16 parametri autenticati (ad esclusione delle quattro eliche del DNA).

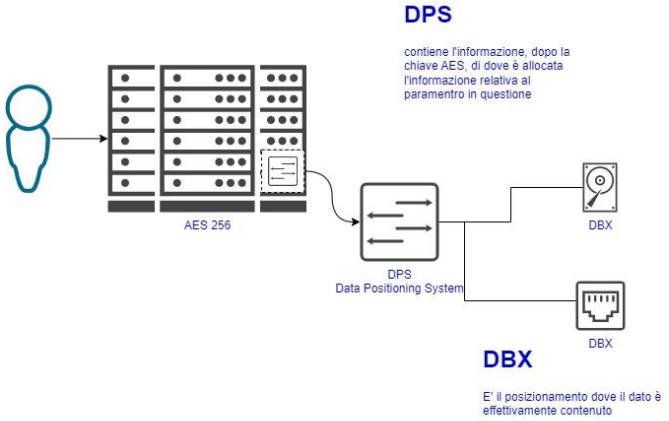
DPS e DBX

Olitec ®© Laboratorio di Ricerca e Sviluppo presso
Fondazione Olitec Caritate Christi - olimaint©® is a trade mark of Olimaint Company
Brescia Via Saleri 55/58 - Italy (EU)
Valmontone via Colle S.Angelo 2/O - Italy (EU)

www.olimaint.tech - desk@oliverso.it

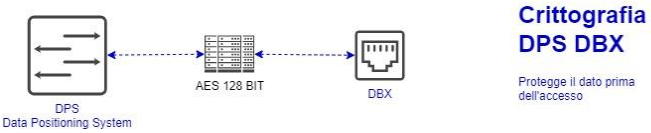
☏ +39 030 364332 int 5 +39 345 563 0496

Il DPS, Data Positioning System, è il puntatore protetto da crittografia AES256 che contiene l'informazione relativa all'esatto posizionamento del dato in forma fisica. Il DPS contiene l'informazione di allocazione mentre il DBX è dove il dato è realmente presente.
I 16 parametri dell'HBA utilizzano DBX diversi uno dall'altro basati su tecnologie complementari ma



non sovrapponibili.

L'apertura di un HBA avvia una Call To Action dove ogni parametro interroga il suo DPS e verifica che il DBX sia quello originariamente inserito e le cui transazioni di modifica nel tempo sono state scritte nella BC che affianca ogni singolo parametro, oltre in quella che affianca l'interno HBA.



Il singolo parametro per essere interrogato nella sua posizione reale e fisicità reale richiede una ulteriore chiave di accesso AES a 128 Bit, più snella, per poter avere accesso all'informazione.

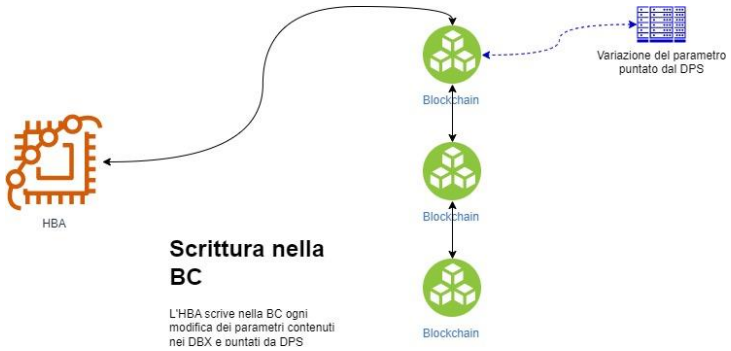
La Blockchain di supporto alle transazioni di modifica del singoli parametri

Ogni modifica all'interno dei 16 parametri dell'HBA viene registrata su 16 BC ognuna delle quali è affiancata al singolo parametro, al modificarsi di un elemento DBX viene effettuata una scrittura sulla relativa BC di riferimento per garantire la correttezza delle informazioni e la veridicità e verificabilità delle stesse.

Olitec ®© Laboratorio di Ricerca e Sviluppo presso
Fondazione Olitec Caritate Christi - olimaint©® is a trade mark of Olimaint Company
Brescia Via Saleri 55/58 - Italy (EU)
Valmontone via Colle S.Angelo 2/O - Italy (EU)

www.olimaint.tech - desk@oliverso.it

☏ +39 030 364332 int 5 +39 345 563 0496



Crittografia Rijndael - AES 128/256

Rijndael è un'evoluzione del primo algoritmo sviluppato da Daemen e Rijmen, Square. Square era stato sviluppato per SHARK.
A differenza del DES, Rijndael è una rete a sostituzione e permutazione, non una rete di Feistel, che implementa comunque il principio crittografico di Shannon di "confusione e diffusione". AES è veloce sia se sviluppato in software sia se sviluppato in hardware, è relativamente semplice da implementare, richiede poca memoria ed offre un buon livello di protezione/sicurezza, motivi che complessivamente l'hanno preferito agli altri algoritmi proposti.
Il nuovo standard di cifratura sta sostituendo i precedenti standard e la sua diffusione continua ad aumentare. Formalmente, AES non è equivalente al Rijndael (sebbene nella pratica siano intercambiabili) dato che il Rijndael gestisce differenti dimensioni di blocchi e di chiavi. Nell'AES il blocco è invece di dimensione fissa (128 bit) e la chiave può essere di 128, 192 o 256 bit mentre il Rijndael specifica solo che il blocco e la chiave devono essere un multiplo di 32 bit con 128 bit come minimo e 256 bit come massimo.
AES opera utilizzando matrici di 4×4 byte chiamate stati (*states*). Quando l'algoritmo ha blocchi di 128 bit in input, la matrice State ha 4 righe e 4 colonne; se il numero di blocchi in input diventa di 32 bit più lungo, viene aggiunta una colonna allo State, e così via fino a 256 bit. In pratica, si divide il numero di bit del blocco in input per 32 e il quoziente specifica il numero di colonne.
C'è un passaggio iniziale:

1. AddRoundKey – Ogni byte della tabella viene combinato con la chiave di sessione, la chiave di sessione viene calcolata dal gestore delle chiavi.

Successivamente per cifrare sono previsti diversi round o cicli di processamento: ogni round (fase) dell'AES (eccetto l'ultimo) consiste dei seguenti quattro passaggi:

1. SubBytes – Sostituzione non lineare di tutti i byte che vengono rimpiazzati secondo una specifica tabella.
2. ShiftRows – Spostamento dei byte di un certo numero di posizioni dipendente dalla riga di appartenenza.

Olitec ®© Laboratorio di Ricerca e Sviluppo presso
Fondazione Olitec Caritate Christi - olimaint©® is a trade mark of Olimaint Company
Brescia Via Saleri 55/58 - Italy (EU)
Valmontone via Colle S.Angelo 2/O - Italy (EU)
www.olimaint.tech - desk@oliverso.it
☏ +39 030 364332 int 5
+39 345 563 0496

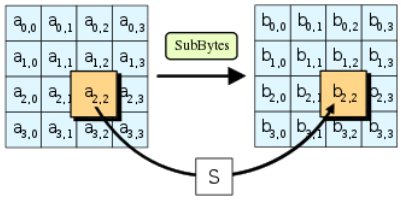
3. MixColumns – Combinazione dei byte con un'operazione lineare, i byte vengono trattati una colonna per volta.
4. AddRoundKey – Ogni byte della tabella viene combinato con la chiave di sessione, la chiave di sessione viene calcolata dal gestore delle chiavi.

Il numero di round o cicli di processamento/elaborazione crittografica dei quattro passaggi precedenti è 10 con l'ultimo round che salta il passaggio MixColumns. A seguito la descrizione di ogni singolo passaggio.

La fase di decifratura non è identica a quella di cifratura dal momento che gli step sono eseguiti in ordine inverso. Tuttavia, si può definire un cifrario inverso equivalente ai passi dell'algoritmo usato per la cifratura, usando la funzione inversa a ogni step e un differente key schedule. Funziona siccome il risultato non cambia quando si scambiano la fase di SubBytes con quella di ShiftRows, e quella di MixColumns con una fase aggiuntiva di AddRoundKey.

SubBytes

Nel passaggio SubBytes ogni byte della matrice viene modificato tramite la S-box a 8 bit. Questa operazione provvede a fornire la non linearità all'algoritmo. La S-box utilizzata è derivata da una funzione inversa nel campo finito GF(2^8), conosciuta per avere delle ottime proprietà di non linearità. Per evitare un potenziale attacco basato sulle proprietà algebriche la S-box è costruita combinando la funzione inversa con una trasformazione affine invertibile. La S-box è stata scelta con cura per non possedere né punti fissi né punti fissi opposti.



Nel passaggio SubBytes, ogni byte della matrice è sostituito con i dati contenuti nella trasformazione S; $b_{ij} = S(a_{ij})$.

ShiftRows

Il passaggio ShiftRows provvede a spostare le righe della matrice di un parametro, e dipende dal numero di riga. Nell'AES la prima riga resta invariata, la seconda viene spostata di un posto verso sinistra, la terza di due posti e la quarta di tre. In questo modo l'ultima colonna dei dati in ingresso andrà a formare la *diagonale* della matrice in uscita. (Rijndael utilizza un disegno leggermente diverso per via delle matrici di lunghezza non fissa.)

Tutte le operazioni sono effettuate utilizzando l'indice della colonna “modulo” il numero di colonne.

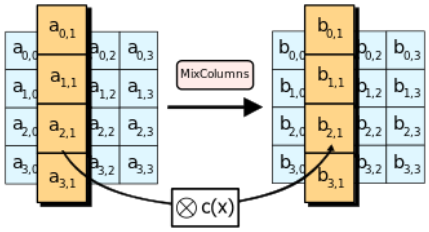
MixColumns

Il passaggio MixColumns prende i quattro byte di ogni colonna e li combina utilizzando una trasformazione lineare invertibile. Utilizzati in congiunzione, ShiftRows e MixColumns provvedono a far rispettare il criterio di confusione e diffusione nell'algoritmo (teoria di Shannon). Ogni colonna è trattata come un polinomio

Olitec ®© Laboratorio di Ricerca e Sviluppo presso
Fondazione Olitec Caritate Christi - olimaint©® is a trade mark of Olimaint Company
Brescia Via Saleri 55/58 - Italy (EU)
Valmontone via Colle S.Angelo 2/O - Italy (EU)

www.olimaint.tech - desk@oliverso.it

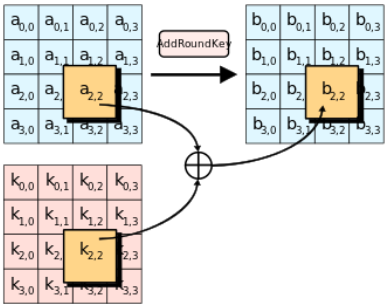
☏ +39 030 364332 int 5 +39 345 563 0496



Nel passaggio MixColumns ogni colonna di byte viene moltiplicata per un polinomio fisso *c(x)*.

AddRoundKey

Il passaggio AddRoundKey combina con uno XOR la chiave di sessione con la matrice ottenuta dai passaggi precedenti (State). Una chiave di sessione viene ricavata dalla chiave primaria ad ogni round (con dei passaggi più o meno semplici, ad esempio uno shift di posizione dei bit) grazie al Key Scheduler.



Nel passaggio AddRoundKeys ogni byte della matrice viene combinato con la sua sottochiave tramite un'operazione di XOR.

Sicurezza della chiave AES

La National Security Agency (NSA) segnalava che tutti i finalisti del processo di standardizzazione erano dotati di una sicurezza sufficiente per diventare l'AES, ma che fu scelto il Rijndael per via della sua flessibilità nel trattare chiavi di lunghezza diversa, per la sua semplice implementazione in hardware e in software e per le sue basse richieste di memoria che ne consentono un'implementazione anche in dispositivi con scarse risorse come le smart card.

L'AES può essere utilizzato per proteggere le informazioni secretate. Per il livello SECRET è sufficiente una chiave a 128 bit mentre per il livello Top secret si consigliano chiavi a 192 o 256 bit. Questo significa che per la prima volta il pubblico ha accesso ad una tecnologia crittografica che NSA ritiene adeguata per proteggere i documenti TOP SECRET. Si è discusso sulla necessità di utilizzare chiavi lunghe (192 o 256 bit) per i documenti TOP SECRET. Alcuni ritengono che questo indichi che l'NSA ha individuato un potenziale attacco che potrebbe forzare una chiave relativamente corta (128 bit), mentre la maggior parte degli esperti ritiene che le raccomandazioni della NSA siano basate principalmente sul volersi garantire un elevato margine di sicurezza per i prossimi decenni contro un potenziale attacco esaustivo.

Olitec ®© Laboratorio di Ricerca e Sviluppo presso
Fondazione Olitec Caritate Christi - olimaint©® is a trade mark of Olimaint Company
Brescia Via Saleri 55/58 - Italy (EU)
Valmontone via Colle S.Angelo 2/O - Italy (EU)

www.olimaint.tech - desk@oliverso.it

☏ +39 030 364332 int 5 +39 345 563 0496

La maggior parte degli algoritmi crittografici viene forzata riducendo il numero di round. L'AES effettua 10 round per la chiave a 128 bit, 12 round per la chiave a 192 bit e 14 round per la chiave a 256 bit. Al 2006, i migliori attacchi sono riusciti a forzare l'AES con 7 round e chiave di 128 bit, 8 round e chiave di 192 bit e 9 round e chiave di 256 bit.

Alcuni crittografi hanno fatto notare che la differenza tra i round effettuati dall'AES e quelli massimi prima che l'algoritmo non sia più forzabile è ridotta (specialmente con chiavi corte). Questi temono che miglioramenti nelle tecniche di analisi possano permettere di forzare l'algoritmo senza verificare tutte le chiavi. Attualmente una ricerca esaustiva è impraticabile: la chiave a 128 bit produce 3,4×1038 combinazioni diverse. Uno dei migliori attacchi a forza bruta è stato svolto dal progetto distributed.net su una chiave a 64 bit per l'algoritmo RC5; l'attacco ha impiegato quasi 5 anni, utilizzando il tempo libero di migliaia di CPU di volontari. Anche considerando che la potenza dei computer aumenta nel tempo, servirà ancora molto tempo prima che una chiave da 128 bit sia attaccabile con il metodo forza bruta. Molte banche mettono a disposizione per l'home banking dei propri clienti chiavi a 256 bit con il risultato che si ottiene una cifratura ben 2^128 volte più sicura di quella a 128 bit sebbene quest'ultima possa considerarsi altamente sicura ed invalicabile dai moderni PC.

Un altro dubbio riguardante l'AES deriva dalla sua struttura matematica. A differenza della maggior parte degli algoritmi a blocchi, per l'AES esiste un'approfondita descrizione matematica . Sebbene non sia mai stata utilizzata per condurre un attacco su misura, questo non esclude che in futuro questa descrizione non venga utilizzata per condurre un attacco basato sulle sue proprietà matematiche.

Nel 2002 l'attacco teorico chiamato attacco XSL annunciato da Nicolas Courtois e Josef Pieprzyk ha mostrato un potenziale punto debole dell'AES (e di altri cifrari). Sebbene l'attacco sia matematicamente corretto, è impraticabile nella realtà per via dell'enorme tempo macchina richiesto per metterlo in pratica. Miglioramenti nell'attacco hanno ridotto il tempo macchina richiesto e quindi, in un futuro, questo attacco potrebbe diventare attuabile. Ultimamente, alcuni esperti hanno fatto delle osservazioni agli autori dell'attacco. Sembra che abbiano commesso degli errori teorici e che, in realtà, le loro stime siano ottimistiche. Allo stato attuale, la reale pericolosità dell'attacco XSL è un punto interrogativo. Comunque, attualmente, l'AES è considerato un algoritmo veloce, sicuro e gli attacchi, fino ad ora presentati, si sono rivelati degli interessanti studi teorici ma di scarsa utilità nella pratica.

In data 1º luglio 2009 è stato pubblicato un attacco correlato alla chiave migliore del metodo forza bruta su tutti i round di AES-256 e AES-192. L'attacco in questione risulta comunque, per stessa ammissione degli autori (come chiarito nelle conclusioni dello studio), essere ancora solo teoricamente realizzabile e non dovrebbe influire in alcun modo sulla sicurezza delle odierne applicazioni che fanno uso di questo cifrario. Secondo Bruce Schneier comunque questa scoperta

Olitec ®© Laboratorio di Ricerca e Sviluppo presso
Fondazione Olitec Caritate Christi - olimaint©® is a trade mark of Olimaint Company
Brescia Via Saleri 55/58 - Italy (EU)
Valmontone via Colle S.Angelo 2/O - Italy (EU)

www.olimaint.tech - desk@oliverso.it

☏ +39 030 364332 int 5 +39 345 563 0496

potrebbe influire negativamente sulla scelta di AES come blocco costitutivo del nuovo algoritmo di hash in fase di definizione SHA-3.

Cifrario MARS

In crittografia il MARS è un cifrario a blocchi che è stato presentato da IBM come candidato al processo di standardizzazione dell'Advanced Encryption Standard. Il MARS è stato selezionato come finalista dell'AES nell'agosto del 1999 dopo che alla conferenza AES2 del marzo 1999 era stato votato come quinto ed ultimo algoritmo finalista. Il gruppo di sviluppatori che ha progettato il MARS include Don Coppersmith, che ha partecipato anche alla creazione del Data Encryption Standard (DES) circa 20 anni prima.

Secondo quanto dichiarato ufficialmente da IBM, il MARS è, insieme al Serpent, uno dei pochi algoritmi finalisti dell'AES specificatamente sviluppati per resistere anche a tecniche di crittanalisi future. Curioso è il fatto che anche il gruppo di sviluppo del Twofish fece una dichiarazione simile per il suo cifrario.

Il MARS opera su blocchi dati di 128 bit e può usare chiavi di lunghezza variabile da 128 a 448 bit (con incrementi di 32 bit). A differenza della maggioranza dei cifrari a blocchi il MARS ha una struttura eterogenea denominata rete di Feistel non bilanciata: ci sono infatti 8 passaggi "in avanti" ed 8 passaggi "indietro". Questi 16 passaggi sono preceduti e seguiti da altri 8 passaggi definiti di "mescolamento" ed indipendenti dalla chiave di cifratura.

Le sotto-chiavi con lunghe sequenze di 1 e 0 possono portare ad attacchi efficienti contro il MARS. I due bit meno significativi delle sotto-chiavi usate nelle operazioni di moltiplicazione nei passaggi interni sono sempre impostate ad 1. Per questo ci sono sempre due input che non sono modificati attraverso il processo moltiplicativo, ed altri due che hanno output fissi (relativamente alla sotto-chiave).

Eli Biham, Bruce Schneier, Bart Preneel, Lars Knudsen ed altri esperti hanno proposto diversi attacchi su versioni del MARS con un numero ridotto di passaggi. Il più efficiente di questi è quello di Kelsey, Kohno e Schneier condotto ad una versione del MARS con 11 passaggi e che sfrutta l'attacco a boomerang: l'attacco permette di violare il cifrario utilizzando 265 testi in chiaro scelti.

Secure Hash Algorithm

Con il termine SHA (acronimo dell'inglese Secure Hash Algorithm) si indica una famiglia di cinque diverse funzioni crittografiche di hash sviluppate a partire dal 1993 dalla National Security Agency (NSA) e pubblicato dal NIST come standard federale dal governo degli USA (FIPS PUB 180-4).

Olitec ®© Laboratorio di Ricerca e Sviluppo presso
Fondazione Olitec Caritate Christi - olimaint©® is a trade mark of Olimaint Company
Brescia Via Saleri 55/58 - Italy (EU)
Valmontone via Colle S.Angelo 2/O - Italy (EU)

www.olimaint.tech - desk@oliverso.it

☏ +39 030 364332 int 5 +39 345 563 0496

Come ogni algoritmo di hash, l'SHA produce un message digest, o "impronta del messaggio", di lunghezza fissa partendo da un messaggio di lunghezza variabile. La sicurezza di un algoritmo di hash risiede nel fatto che la funzione non sia invertibile (non sia cioè possibile risalire al messaggio originale conoscendo solo questo dato) e che non deve essere mai possibile creare intenzionalmente due messaggi diversi con lo stesso digest. Gli algoritmi della famiglia sono denominati SHA-1, SHA-224, SHA-256, SHA-384 e SHA-512: le ultime 4 varianti sono spesso indicate genericamente come SHA-2, per distinguerle dal primo. Il primo produce un digest del messaggio di soli 160 bit, mentre gli altri producono digest di lunghezza in bit pari al numero indicato nella loro sigla (SHA-256 produce un digest di 256 bit). L'SHA-1 è il più diffuso algoritmo della famiglia SHA ed è utilizzato in numerose applicazioni e protocolli nonostante sia ormai insicuro e verrà presto sostituito dagli altri, più moderni ed efficienti.

La sicurezza di SHA-1 è stata appunto compromessa dai crittoanalisti. Sebbene non siano ancora noti attacchi alle varianti SHA-2, esse hanno un algoritmo simile a quello di SHA-1 per cui sono in atto sforzi per sviluppare algoritmi di hashing alternativi e migliorati. Un concorso aperto per la realizzazione di una nuova funzione SHA-3 venne annunciato nel Federal Register il 2 novembre 2007 dal NIST e attraverso una competizione pubblica, simile a quella adottata per il processo di sviluppo dell'AES,ha portato in data 2 ottobre 2012 ad annunciare come vincitore l'algoritmo Keccak. Opera di un team di analisti italiani e belgi, il Keccak sembra dunque destinato a venire gradualmente incluso e adottato nelle soluzioni di sicurezza informatica più variegate.

Il 23 febbraio 2017 un team di Google ha annunciato la prima tecnica pratica per generare una collisione hash.

La funzione di hash o funzione hash produce una sequenza di bit, detta digest, (o una stringa) strettamente correlata con i dati in ingresso. La parola viene dal termine inglese hash, dal verbo to hash, ovvero sminuzzare, pasticciare, che designa originariamente una polpettina fatta di avanzi di carne e verdure; per estensione, indica un composto eterogeneo cui viene data una forma incerta: "To make a hash of something" vuol dire, infatti, creare confusione, o fare una cosa piuttosto male.

Nel linguaggio matematico e informatico, l'hash è una funzione non invertibile che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza predefinita. Esistono numerosi algoritmi che realizzano funzioni hash con particolari proprietà che dipendono dall'applicazione.

Nelle applicazioni crittografiche si chiede, per esempio, che la funzione hash abbia le seguenti proprietà:

Olitec ®© Laboratorio di Ricerca e Sviluppo presso
Fondazione Olitec Caritate Christi - olimaint©® is a trade mark of Olimaint Company
Brescia Via Saleri 55/58 - Italy (EU)
Valmontone via Colle S.Angelo 2/O - Italy (EU)

www.olimaint.tech - desk@oliverso.it

☏ +39 030 364332 int 5 +39 345 563 0496

resistenza alla preimmagine: sia computazionalmente intrattabile la ricerca di una stringa in input che dia un hash uguale a un dato hash;
resistenza alla seconda preimmagine: sia computazionalmente intrattabile la ricerca di una stringa in input che dia un hash uguale a quello di una data stringa;
resistenza alle collisioni: sia computazionalmente intrattabile la ricerca di una coppia di stringhe in input che diano lo stesso hash.
Nelle applicazioni di basi di dati la funzione hash è usata per realizzare una particolare struttura dati chiamata hash table. In questa applicazione non occorrono proprietà crittografiche e generalmente l'unica proprietà richiesta è che non ci siano hash più probabili di altri.

L'algoritmo di hash elabora qualunque mole di bit (in informatica si dice che elabora dati "grezzi"). Si tratta di una famiglia di algoritmi che soddisfa questi requisiti:

L'algoritmo restituisce una stringa di numeri e lettere a partire da un qualsiasi flusso di bit di qualsiasi dimensione (può essere un file, ma anche una stringa). L'output è detto digest.
L'algoritmo non è invertibile, ossia non è possibile ricostruire il documento originale a partire dalla stringa che viene restituita in output ovvero è una funzione unidirezionale, quest'ultima caratteristica non è indispensabile se si usano gli hash per controllare gli errori nei trasferimenti dei dati, dove le eventuali funzioni di criptaggio possono venir svolte in altre aree del protocollo.
Non esiste una corrispondenza biunivoca tra l'hash e il testo. Dato che i testi possibili, con dimensione finita maggiore dell'hash, sono più degli hash possibili, per il principio dei cassetti ad almeno un hash corrisponderanno più testi possibili. Quando due testi producono lo stesso hash, si parla di collisione, e la qualità di una funzione di hash è misurata direttamente in base alla difficoltà nell'individuare due testi che generino una collisione. Per sconsigliare l'utilizzo di algoritmi di hashing in passato considerati sicuri è stato infatti sufficiente che un singolo gruppo di ricercatori riuscisse a generare una collisione. Questo è quello che è avvenuto ad esempio per gli algoritmi SNEFRU, MD2, MD4, MD5 e SHA-1.

Un hash crittograficamente sicuro non dovrebbe permettere di risalire, in un tempo confrontabile con l'utilizzo dell'hash stesso, ad un testo che possa generarlo.
La lunghezza dei valori di hash varia a seconda degli algoritmi utilizzati. Il valore più comunemente adottato è di 128 bit, che offre una buona affidabilità in uno spazio relativamente ridotto. Tuttavia va registrata la possibilità d'uso di hash di dimensione maggiore (SHA, ad esempio, può anche fornire stringhe di 224, 256, 384 e 512 bit) e minore (che però è fortemente sconsigliato).

Le funzioni hash svolgono un ruolo essenziale nella crittografia: sono utili per verificare l'integrità di un messaggio, poiché l'esecuzione dell'algoritmo su un testo anche minimamente modificato fornisce un message digest completamente differente rispetto a quello calcolato sul testo originale, rivelando la tentata modifica.

Olitec ®© Laboratorio di Ricerca e Sviluppo presso
Fondazione Olitec Caritate Christi - olimaint©® is a trade mark of Olimaint Company
Brescia Via Saleri 55/58 - Italy (EU)
Valmontone via Colle S.Angelo 2/O - Italy (EU)

www.olimaint.tech - desk@oliverso.it

☏ +39 030 364332 int 5 +39 345 563 0496

Le funzioni di hash possono essere anche utilizzate per la creazione di firme digitali, in quanto permettono la rapida creazione della firma anche per file di grosse dimensioni, senza richiedere calcoli lunghi e complessi: è infatti computazionalmente più conveniente eseguire con rapidità un hashing del testo da firmare, e poi autenticare solo quello, evitando così l'esecuzione dei complessi algoritmi di crittografia asimmetrica su moli di dati molto grandi.

La firma digitale è definita come il digest di un documento che poi viene crittografato con chiave privata (e non con quella pubblica, come avviene di solito). La firma digitale è l'unico caso in cui l'uso delle chiavi è invertito: la chiave pubblica serve a decrittare la firma e trovare poi il digest iniziale attraverso l'hash, mentre quella privata serve a crittografare una stringa anziché ad aprirla.

Un ulteriore uso delle funzioni di hash si ha nella derivazione di chiavi da password o passphrase: a partire da un valore arbitrario in ingresso (una stringa o un array di larghe dimensioni) si deriva in modo crittograficamente sicuro (ovvero non è possibile abbreviare il calcolo con una qualche scorciatoia) una chiave di dimensioni adatte alla cifratura. È appena il caso di dire, tuttavia, che a meno di prendere debite contromisure (come l'uso di un salt crittografico), l'utilità di questa procedura è esclusivamente pratica: infatti la sicurezza della chiave derivata è equivalente a quella della stringa di ingresso ai fini di un attacco a dizionario. Di contro, è certamente più comodo per un essere umano ricordare una stringa piuttosto che una lunga sequenza numerica.
Nel contesto delle funzioni hash, ci si riferisce a diversi concetti di sicurezza:

Sicurezza debole: dato un messaggio M, è computazionalmente "difficile" trovare un secondo messaggio M' tale che h(M)=h(M').
Sicurezza forte: è computazionalmente "difficile" trovare una coppia di messaggi M,M' tali che h(M)=h(M').
Questi due concetti di sicurezza vengono distinti anche per via degli effetti che essi possono produrre nel caso in cui ne siano privi: per quanto riguarda ad esempio la possibilità di effettuare una firma digitale, un algoritmo che non garantisca la sicurezza forte, ma quella debole, sarebbe comunque utile dal momento che il messaggio M non può essere "controllato" e bisognerebbe quindi trovare un secondo messaggio M' con uguale funzione di hash, il che sarebbe appunto computazionalmente difficile.
È possibile utilizzare le funzioni di hash per creare una hash table, che è una struttura dati molto efficiente per le operazioni di ricerca. La hash table contiene dati associati ad una chiave di ricerca e viene spesso utilizzato nei database per indicizzare gli elementi che saranno oggetto di ricerca. Questa tecnica (detta di hashing) permette di realizzare funzioni di ricerca che riescono ad individuare l'elemento desiderato in un tempo costante, indipendente (almeno in teoria) dal numero di elementi presenti nell'indice.

L'uso delle funzioni hash per trovare errori nelle trasmissioni è molto comune. La funzione hash viene calcolata dal mittente a partire dai dati e il suo valore è inviato insieme ai dati. Il ricevente calcola di

Olitec ®© Laboratorio di Ricerca e Sviluppo presso
Fondazione Olitec Caritate Christi - olimaint©® is a trade mark of Olimaint Company
Brescia Via Saleri 55/58 - Italy (EU)
Valmontone via Colle S.Angelo 2/O - Italy (EU)

www.olimaint.tech - desk@oliverso.it

☏ +39 030 364332 int 5 +39 345 563 0496

nuovo la funzione hash, e se i valori hash non corrispondono, significa che è avvenuto un errore durante la trasmissione. Questo metodo consente un controllo dell'integrità dei dati migliore della più tradizionale checksum.

Gli algoritmi di hash, in particolare SHA1 e MD5, sono largamente utilizzati nell'ambito dell'informatica forense per validare e in qualche modo "firmare" digitalmente i dati acquisiti, tipicamente le copie forensi. La recente legislazione impone infatti una catena di custodia che permetta di preservare i reperti informatici da eventuali modifiche successive all'acquisizione: tramite i codici hash è possibile in ogni momento verificare che quanto repertato sia rimasto immutato nel tempo. Se i codici hash corrispondono, entrambe le parti in un procedimento giudiziario hanno la ragionevole certezza di lavorare sulla stessa versione dei reperti, garantendo quindi una uniformità di analisi e in genere di risultati. I risultati dei codici hash vengono ormai calcolati di default dalla maggioranza dei software per acquisizione forense e allegati alle copie forensi salvate.

Attacco XSL su HBA - L'impenetrabilità dell'HBA

In crittografia, l'attacco eXtended Sparse Linearization (XSL) è un metodo teorico di crittoanalisi per i cifrari a blocchi, pubblicato per la prima volta nel 2002 dai ricercatori Nicolas Courtois e Josef Pieprzyk.

Questo nuovo approccio ha suscitato qualche polemica tra gli esperti di crittoanalisi perché si sosteneva che fosse in grado di rompere il cifrario Advanced Encryption Standard (AES), noto anche come Rijndael, più velocemente di una ricerca esaustiva (brute force). Poiché l'AES è uno standard di cifratura accreditato dal NIST , ed è già ampiamente utilizzato in ambito commerciale e governativo per la trasmissione di informazioni riservate e segrete, trovare una tecnica in grado di ridurre il tempo necessario per recuperare il messaggio segreto senza disporre della chiave potrebbe avere implicazioni considerevoli.

Nel caso generale, la risoluzione di equazioni polinomiali quadratiche su un insieme finito di numeri è un problema NP-difficile con diverse applicazioni in crittografia. L'attacco XSL richiede de facto un algoritmo efficiente per affrontare le equazioni polinomiali quadratiche.

Nel 1999, Kipnis e Shamir hanno dimostrato che un particolare algoritmo a chiave pubblica, noto come schema Hidden Field Equations (HFE), poteva essere ridotto a un sistema con più equazioni quadratiche che incognite. Una tecnica per risolvere tali sistemi è la linearizzazione, che prevede la sostituzione di ogni termine quadratico con una variabile indipendente e la risoluzione del sistema lineare risultante mediante un algoritmo come l'eliminazione gaussiana. Per avere successo, la linearizzazione richiede un numero sufficiente di equazioni linearmente indipendenti (approssimativamente pari al numero di termini). Tuttavia, per la crittoanalisi di HFE le equazioni

Olitec ®© Laboratorio di Ricerca e Sviluppo presso
Fondazione Olitec Caritate Christi - olimaint©® is a trade mark of Olimaint Company
Brescia Via Saleri 55/58 - Italy (EU)
Valmontone via Colle S.Angelo 2/O - Italy (EU)

www.olimaint.tech - desk@oliverso.it

☏ +39 030 364332 int 5 +39 345 563 0496

erano troppo poche, quindi Kipnis e Shamir proposero la ri-linearizzazione, una tecnica in cui dopo la linearizzazione vengono aggiunte altre equazioni non lineari e il sistema risultante viene risolto con una seconda applicazione della linearizzazione. La ri-linearizzazione si è dimostrata abbastanza generale da poter essere applicata ad altri schemi.

Nel 2000, un gruppo di ricerca guidato da Courtois ha proposto un algoritmo migliorato per la risoluzione di equazioni polinomiali quadratiche noto come XL (eXtended Linearization), che aumenta il numero di equazioni moltiplicandole con tutti i monomi di un certo grado. Le stime di complessità hanno mostrato che l'attacco XL non avrebbe funzionato contro le equazioni derivate da cifrari a blocchi come AES . Tuttavia, i sistemi di equazioni prodotti avevano una struttura particolare e l'algoritmo XSL è stato sviluppato come un perfezionamento di XL in grado di sfruttare questa struttura. In XSL, le equazioni sono moltiplicate solo per monomi accuratamente selezionati.
L'algoritmo scelto per sfruttare l'attacco XSL non influisce sulla sicurezza reale dei cifrari a blocchi, dato che il metodo ha un fattore di lavoro elevato per via dell'enorme tempo macchina richiesto per l'esecuzione. Ciò significa che questo attacco non riduce effettivamente lo sforzo di violare AES attraverso ricerca esaustiva. Ciononostante, l'attacco ha fatto sì che alcuni esperti esprimessero un maggiore disagio nei confronti della semplicità algebrica dell'attuale AES .

In sintesi, l'attacco XSL si basa sull'analisi degli interni di un cifrario e sulla derivazione di un sistema di equazioni quadratiche simultanee. Questi sistemi di equazioni sono tipicamente molto grandi nell'utilizzo dello standard AES, sfruttando ad esempio 8000 equazioni con 1600 variabili per l'AES a 128 bit. Sono noti diversi metodi per risolvere tali sistemi , sebbene questi possano risultare complessi nell'implementazione pratica . Nell'attacco XSL l'applicazione di questi metodi risolutivi risulta tediosa con l'aumentare della lunghezza in bit della chiave di cifratura scelta, come riportato anche nell'Abstract della pubblicazione di Courtois e Pieprzyk.

Olitec ®© Laboratorio di Ricerca e Sviluppo presso
Fondazione Olitec Caritate Christi - olimaint©® is a trade mark of Olimaint Company
Brescia Via Saleri 55/58 - Italy (EU)
Valmontone via Colle S.Angelo 2/O - Italy (EU)

www.olimaint.tech - desk@oliverso.it

☏ +39 030 364332 int 5 +39 345 563 0496

L'estensore della guida : Nicolini Massimiliano

Ricercatore in scienze dell'informazione, specializzato VRO – la tecnologia alla base del metaverso – e intelligenza artificiale, Massimiliano Nicolini è membro italiano del Metaverse Standards Forum, organizzazione che promuove lo sviluppo di uno standard di interoperabilità volto a garantire un metaverso aperto e inclusivo.

In qualità di Software Engineer – iA specialist, da oltre 25 anni dirige il dipartimento ricerca e sviluppo sulle intelligenze artificiali e VRO di Olimaint, società di informatica nata nel 1981 e specializzata nello sviluppo di soluzioni per piccole, medie e grandi aziende commerciali ed industriali, che è stata la prima al mondo nello sviluppo di molteplici applicazioni in VRO (sanità, commercio, protezione, turismo, cultura, e molti altri), *dipartimento oggi confluito in Fondazione Olitec fortemente voluta dalla famiglia per onorare Giovanni Nicolini, al quale, sono intitolati cinque centri di ricerca, un percorso accademico alla Kotler University, un'ala del museo di arte moderna "Farm Cultural Park.*

Scelto dall'artista Fra Sidival Fila OFM, uno dei virtuosi del Pantheon, per realizzare il primo metaverso artistico di un religioso al mondo.

Philip Kotler, il padre del marketing moderno, lo ha scelto per la creazione dei sistemi di formazione del marketing web3 ritenendolo *"l'unico in grado di creare una realtà digitale efficace e per nulla distinguibile dal reale", è citato, unico italiano, in Essential of Modern Marketing.*

Ha realizzato la prima applicazione al mondo per lo svolgimento di attività politiche coordinate col mondo reale durante l'evento la politica nel metaverso al Tempio di Adriano in Roma nel maggio 2022 con l'allora premier.

E' l'autore della 8° legge istitutiva del metaverso recepita a livello internazionale.

E' uno degli istitutori del programma di formazione Magellano, unitamente a ricercatori internazionali ed a Philip Kotler che lo ha scelto per la realizzazione della prima scuola di marketing nel metaverso.

Membro del comitato scientifico di Grandi Ospedali.

Membro del comitato scientifico di METIT (associazione italiana professionale del metaverso)

Olitec ®© Laboratorio di Ricerca e Sviluppo presso
Fondazione Olitec Caritate Christi - olimaint©® is a trade mark of Olimaint Company
Brescia Via Saleri 55/58 - Italy (EU)
Valmontone via Colle S.Angelo 2/O - Italy (EU)

www.olimaint.tech - desk@oliverso.it

☏ +39 030 364332 int 5 +39 345 563 0496

Analista nel campo degli algoritmi non deterministici, ha collaborato in qualità di "Esperto Esterno in Audizione" con la I° commissione affari costituzionali del Senato della Repubblica italiana (aff. 1144) sul tema metaverso ed è l'autore dell'8° legge istitutiva del metaverso, recepita dal consorzio internazionale T42.

È membro del comitato scientifico per lo studio del metaverso di Fondazione Leonardo CDM sotto la direzione di presidenza dell'on Luciano Violante per l'analisi VRO dal Febbraio 2023.

A Marzo 2023 è stato inserito tra le 100 personalità a livello globale fautori del cambiamento dal comitato di valutazione dell'WMS (World Marketing Summit), insieme a capi di stato, premi nobel e grandi personaggi della storia e della civiltà contemporanea.

Da luglio 2023 e membro di PA Social, gruppo di studio per la transizione digitale della pubblica amministrazione.

E' autore di diversi romanzi e saggi scientifici, alcuni dei quali distribuiti da Feltrinelli.

E' firmatario dei brevetti Argo ®, Galileo Analisys ®, OPM Y7®, OPM SF21®, OPM VK1®, OPM B1®, OPM TN1®, XPL VRO IMMERSIVE PROTOCOL ®, Gedoca®, Oliversive Visore Immersive®, Human Biometric Avatar HBA ®.

E' firmatario del protocollo di interoperabilità stabilito dal Metaverse Standard Forum dal titolo "Interoperabilità globale nella VRO – USD GLFT GLB" emesso nel 2022.

Olitec ®© Laboratorio di Ricerca e Sviluppo presso
Fondazione Olitec Caritate Christi - olimaint©® is a trade mark of Olimaint Company
Brescia Via Saleri 55/58 - Italy (EU)
Valmontone via Colle S.Angelo 2/O - Italy (EU)

www.olimaint.tech - desk@oliverso.it

☏ +39 030 364332 int 5 +39 345 563 0496