

Libro Bianco di Elastos

Smart-web supportato dalla blockchain

Disposto dalla Fondazione Elastos

1 gennaio 2018

Descrizione

Questo documento è la versione 0.2 del Libro Bianco di Elastos, che integra la descrizione degli obiettivi strategici di Elastos ed il piano di sviluppo tecnologico. Elastos continuerà ad aggiornare questo Libro Bianco per riflettere i nuovi sviluppi. Per le più recenti informazioni sul Libro Bianco di Elastos, la tabella di marcia, il team, la gestione della fondazione, gli investitori ed i partner strategici la invitiamo a visitare il sito Web ufficiale di Elastos

<https://www.elastos.org/>

Contatti

Fondazione Elastos:

Elastos (Shanghai):

The 11th floor, Huahong International Building

No. 463 the Tanggu Road, Hongkou District

Shanghai, Cina 200080

Elastos (Beijing):

Plug & Play, Building G,

Zhongguancun Yingzao Street

No. 45 Chengfu Road, Haidian District

Beijing, China 100084

Email:

Il gruppo del Libro Bianco: whitepaper@elastos.org

La comunità globale: global-community@elastos.org

Relazioni pubbliche: pr@elastos.org

Relazioni con gli investitori: ir@elastos.org

Il comitato di Elastos: elastos-council@elastos.org

Altre relazioni: contact@elastos.org

La Fondazione Elastos è registrata a Singapore.

Il copyright di questo documento è di proprietà della Elastos Foundation e tutti i diritti sono riservati.

Avviso di copyright

La Fondazione Elastos ha tutti i diritti su questo documento.

Disconoscimento

Elastos svilupperà di continuo la sua tecnologia e la sua struttura organizzativa, mantenendo gli attuali principi guida sulla comunità Elastos ed il piano di assegnazione dei token Elastos.

- **Introduzione ad Elastos**

Elastos mira a creare un nuovo tipo di Internet, alimentato dalla tecnologia blockchain.

Con questo nuovo Internet, le persone saranno in grado di possedere risorse digitali e creare ricchezza da esse. Oggi, apparentemente c'è una offerta illimitata di libri digitali, film, musica e giochi. Ma non necessariamente le persone possiedono le relative proprietà digitali. Puoi comprare un libro digitale, ad esempio, ma non lo puoi vendere a nessun altro. Quindi, è un possesso reale ? Elastos vuole rendere i beni digitali scarsi, identificabili e negoziabili. I diritti di proprietà aprono la strada alla creazione di ricchezza ed Elastos vuole costruire un nuovo World Wide Web che rispetti tali diritti.

L'obiettivo è creare un Internet che permetta agli utenti di accedere direttamente a contratti, film e giochi, senza dover passare attraverso un lettore multimediale o un'altra piattaforma intermedia. Elastos intende usare la tecnologia blockchain per identificare con un'ID i contenuti digitali, rendendo possibile sapere chi possiede quali risorse digitali. Attraverso l'Internet di Elastos, i registi sapranno quante volte i loro film sono stati guardati. La combinazione di Elastos e la tecnologia blockchain pone le fondamenta per un'Internet del Valore, affidabile e sicuro.

Elastos sarà una piattaforma per applicazioni decentralizzate (Dapps) che funziona su una rete peer-to-peer senza controllo centralizzato. Le persone potranno accedere a queste Dapps con il loro smartphone, senza dovere cambiare il proprio sistema operativo. Il vecchio Internet è una Rete di informazioni. Se tu fai clic un URL, ricevi dati. Elastos sta creando una Rete per le applicazioni. Quando fai clic su un URL, ricevi il codice. La rete di Elastos si comporterà come una zona economica speciale dove i token di Elastos vengono utilizzati come valuta di base.

Elastos è un software open-source il cui sviluppo è stato sponsorizzato da giganti industriali come Tsinghua Science Park, TD-SCMA Industrial Alliance e la Foxconn Group con più di 200 milioni RMB (yuan cinese). Elastos ha pubblicato più di 10 milioni di righe di codice sorgente, inclusi 4 milioni di righe di codice sorgente originale.

2 Il contesto tecnologico

La Blockchain di Bitcoin è un registro decentralizzato ed immutabile che consente alle persone di riporre la loro fiducia sui dati. Ethereum ha realizzato una blockchain programmabile che può supportare smart contracts (contratti intelligenti), consentendo alle persone di riporre la loro fiducia sul codice. I smart contracts, in parole povere, permettono alle transazioni di eseguirsi automaticamente una volta soddisfatti gli obblighi contrattuali. I venditori verranno pagati solo, ad esempio, dopo che i loro

prodotti sono stati ricevuti dagli acquirenti. Le aziende interessate a raccogliere finanziamenti possono eseguire compiti di produzione specifici solo dopo aver raccolto una certa quantità di fondi. In caso contrario, gli stessi saranno restituiti ai partecipanti.

Grazie agli smart contracts, non dobbiamo preoccuparci delle violazioni del contratto o dell'affidabilità creditizia dei nostri partner commerciali, perché la blockchain eseguirà le transazioni dopo che entrambe le parti avranno rispettato le loro promesse. Questo sistema elimina la mancanza di fiducia tra gli acquirenti e venditori. La domanda è: come possiamo applicare questo sistema di smart contracts ad un insieme ancora più ampio di imprese? Potremmo usarlo per gestire una libreria elettronica o una piattaforma di trading per videogiochi o film?

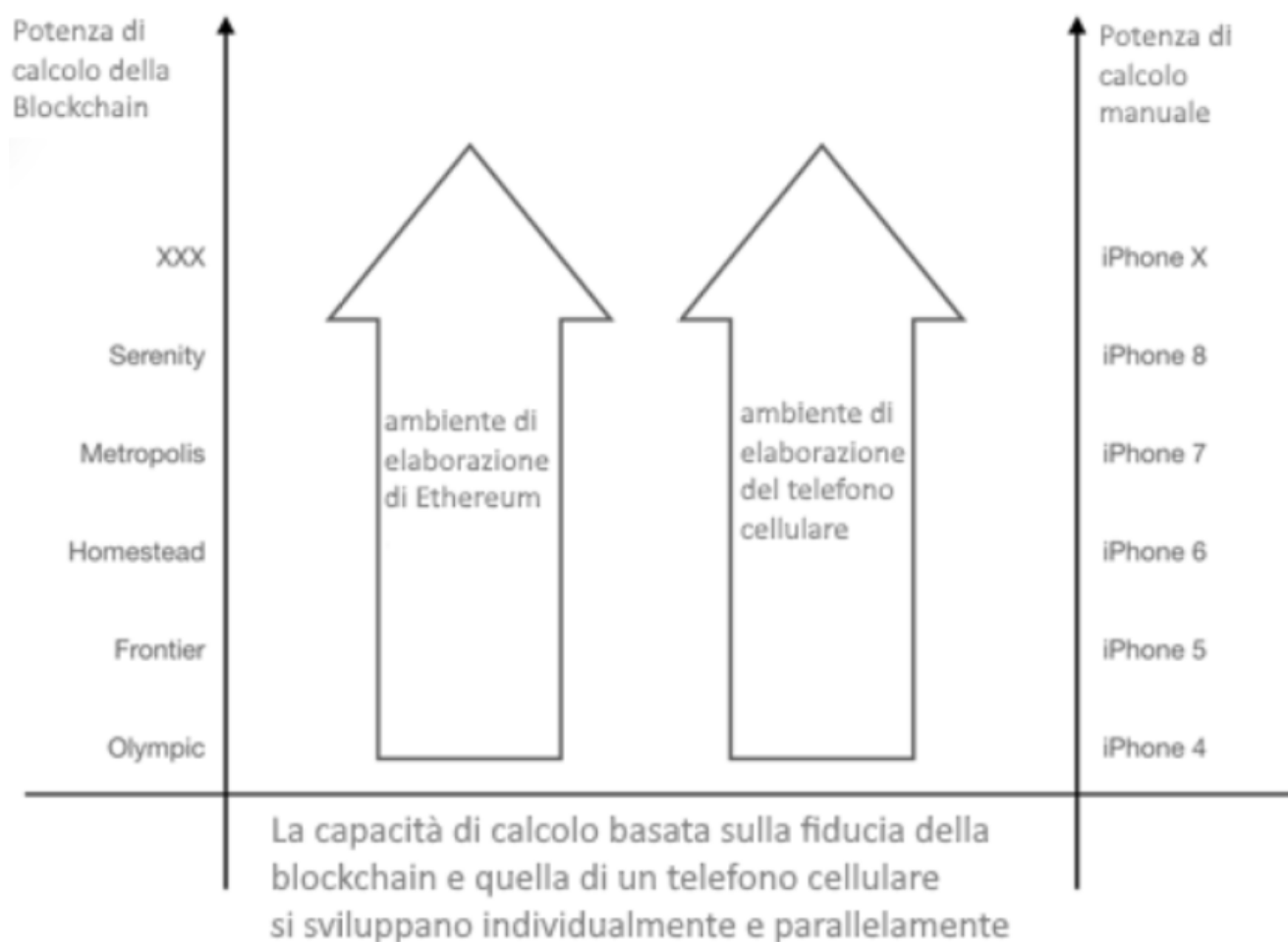
Gli smart contracts di Ethereum sono utili quando applicati a progetti finanziari e semi-finanziari, così come al voto online. Tuttavia Elastos ritiene che le applicazioni decentralizzate basate sul Ethereum hanno le seguenti limitazioni:

- Archiviazione e velocità. La capacità di archiviazione è limitata alla stessa blockchain, infatti può salvare solo una quantità limitata di dati con una velocità molto bassa. La popolarità del gioco su blockchain CryptoKitties ha causato la congestione di Ethereum, evidenziando la difficoltà di eseguire smart contracts unicamente sulla principale blockchain pubblica.
- Falle nel codice (*bugs*). Gli smart contracts non sono né bloccabili né revisionabili una volta eseguiti. Questo è logico e protegge entrambe le parti: poiché contrattualmente pattuiti non possono essere fermati o modificati. Permangono però alcuni difetti insiti negli smart contracts, come gli attacchi all'organizzazione autonoma decentralizzata (*DAO attacks*). Per lo più, non esiste un modo di dimostrare che un programma non sia affetto da errori.
- Costo. Attualmente, gli smart contracts, la registrazione dei dati e l'esecuzione dei contratti sono tutti condotti sulla blockchain. Ciò significa che molti nodi eseguono ripetutamente lo stesso compito. Ethereum richiede che ogni volta che svolgi un'attività, paghi una commissione. Per questo motivo l'esecuzione dei contratti su Ethereum può diventare onerosa.
- Dati spazzatura. C'è un accumulo di dati spazzatura cronologici sulla blockchain di Ethereum. Una volta pubblicato, uno smart contract verrà salvato per sempre nella blockchain. I dati indesiderati e ridondanti hanno un'influenza negativa sull'efficienza della blockchain e questo può portare alla congestione di Ethereum.
- Mancanza di flessibilità. L'accoppiamento tra la blockchain e la macchina virtuale di Ethereum (EVM) che esegue smart contracts li rende inseparabili. Gli

aggiornamenti alla blockchain influiscono la macchina virtuale di Ethereum e viceversa.

- Sicurezza. Gli smart contracts in esecuzione su sistemi Ethereum o simili ad Ethereum sono soggetti a *middleman attacks* quando fuoriescono dalla blockchain e su altri siti Web.

A causa dei problemi sopra menzionati, Elastos crede che sia difficile e sconveniente per gli utenti leggere libri digitali, giocare e utilizzare chat protette dalla crittografia utilizzando gli smart contracts di Ethereum. Inoltre le persone sono abituate ad utilizzare i loro telefoni cellulari per eseguire le applicazioni. Elastos vuole che gli utenti siano in grado di accedere all'innovativo sistema basato sulla fiducia offerto dalla blockchain tramite i dispositivi mobili già in loro possesso.



Come dimostra l'illustrazione qui sopra, a prescindere dalla potenza del telefono

cellulare dell'utente, questo non sarà in grado di migliorare la velocità di elaborazione di Ethereum. Non importa quanti aggiornamenti di Ethereum ci siano, la sua garantita affidabilità non si estende all'utilizzo quotidiano del telefono cellulare. Questo è dovuto al fatto che la potenza di calcolo di Ethereum e quella dei telefoni cellulari furono sviluppate ed applicate in parallelo e non integrate.

Gli smart contracts di oggi sono progettati per funzionare esclusivamente sulla blockchain. Elastos eseguirà le applicazioni decentralizzate che sono supportate dalla tecnologia blockchain, ma non devono essere necessariamente eseguite sulla blockchain stessa. Elastos consentirà agli utenti di accedere a tali applicazioni decentralizzate tramite i loro attuali sistemi operativi senza doverli sostituire. Le applicazioni decentralizzate si eseguiranno via Elastos Runtime, che funziona su Android, iOS o PC.

In sintesi, Ethereum è ottimo per gli smart contracts ma Elastos crede che ci siano due ragioni principali per cui la macchina virtuale di Ethereum non è adatta per l'esecuzione delle applicazioni decentralizzate:

- Le bockchains sono create per il mantenimento dei registri basato sul consenso, ma possono essere prive di una adeguata velocità di calcolo o di flessibilità.
- Le attuali blockchain sono progettate per registrare le transazioni, non per immagazzinare dati. Semplicemente non c'è abbastanza spazio sulla blockchain attuale per archiviare una grande quantità di film e libri digitali.

Per affrontare il primo problema, Elastos propone di adottare una struttura con una blockchain principale flessibile ed una blockchain secondaria, chiamate rispettivamente *mainchain* e *sidechain*. La catena principale è responsabile soltanto delle transazioni di base e del trasferimento dei pagamenti, la catena secondaria esegue gli smart contracts per supportare varie applicazioni e servizi.

Per affrontare il secondo problema, Elastos intende eseguire le applicazioni stesse sull'Elastos Runtime anziché su una blockchain già congestionata. Questo metodo si rivela essere anche più sicuro. Con Elastos, tutti i dati di rete devono essere inviati attraverso un canale affidabile ed identificabile. L'identificazione e l'autenticazione provengono direttamente dalla ID fornita dalla blockchain. In questo modo, l'affidabilità stessa della blockchain può essere trasferita ad Elastos Runtime. Elastos Runtime può avere varie forme: un sistema operativo indipendente, una macchina virtuale o un kit di sviluppo software (SDK) che si integra in app native di altri sistemi operativi tradizionali.

La filosofia alla base del design di Elastos integra la praticità dei telefoni cellulari con la affidabilità della tecnologia blockchain, permettendo agli utenti di accedere alle applicazioni senza passare attraverso un intermediario di terze parti. Elastos creerà un

ambiente in cui le risorse digitali potranno essere scambiate peer to peer.

- **Elastos: Una rete mondiale alimentata dalla blockchain**

La filosofia di Elastos è nata da Rong Chen, ex ingegnere informatico senior di Microsoft. Basandosi sulla sua esperienza in Microsoft, Chen ha ipotizzato una piattaforma in cui ad applicazioni e servizi non è permesso di accedere direttamente a Internet. Senza accesso alla rete, un software malevolo non sarebbe in grado di accedere ai dati agli utenti o attaccare altri servizi su Internet. La visione di Chen è stata successivamente sviluppata in un sistema operativo snello ed aperto per le macchine virtuali (github.com/Elastos). Nel 2017, la tecnologia blockchain è stata inclusa nella visione di Chen, consentendo lo sviluppo di Elastos Smart Web (Rete intelligente di Elastos).

Elastos Smart Web è composto da quattro pilastri:

- La Blockchain di Elastos. Elastos intende costruire una Smart Web decentralizzata, dove ogni dispositivo, individuo, sito Web o risorsa digitale ha un ID certificato. La tecnologia blockchain consente di creare una rete internet basata sulla fiducia.
- Elastos Runtime. Elastos Runtime è un sistema operativo snello che impedisce ad applicazioni e servizi di accedere direttamente ad Internet. Elastos Runtime viene eseguito sul dispositivo mobile o sul PC del cliente.
- Elastos Carrier. È una piattaforma peer-to-peer completamente decentralizzata. La funzione del carrier è quella di indirizzare tutto il traffico di rete tra macchine virtuali e trasmette informazioni per conto delle applicazioni.
- Kit di sviluppo del software di Elastos (SDK). Le applicazioni richiedono che l'Elastos SDK acceda ai loro ID e ai servizi Elastos Carrier sullo Smart Web.

Elastos ha le seguenti caratteristiche:

- La catena pubblica Elastos è semplice, lineare ed è invisibile ad applicazioni e servizi di terze parti.
- Elastos previene il sovraccarico della blockchain principale con alcune catene secondarie predefinite ed integrate nella piattaforma Elastos Carrier.
- Elastos promuove i diritti di proprietà dei contenuti digitali. Elastos ha la capacità di rilasciare token per risorse digitali o per applicazioni e stabilire il diritto di proprietà dei contenuti digitali tramite smart contracts.
- Elastos Runtime viene eseguito sul sistema operativo dei dispositivi mobili dei clienti. Le applicazioni sono gratuite e le loro prestazioni sono equivalenti alle applicazioni mobili esistenti. Elastos supporta i linguaggi di programmazione

tradizionali, rendendo relativamente facile la scrittura dei codici. Elastos supporta anche i framework di programmazione più conosciuti.

- La separazione delle app dalla rete ha il vantaggio di garantire che i contenuti digitali non fuoriescano.
- Anche quando le applicazioni di Elastos sono in esecuzione su sistemi operativi tradizionali come iOS, Android e Windows, il sistema operativo locale non sarà in grado di manomettere i diritti di proprietà delle risorse digitali. Il valore delle risorse digitali è quindi mantenuto.
- Per le applicazioni non Elastos come le applicazioni Android o iOS, gli utenti possono accedere ad Elastos Smart Web tramite l'SDK di Elastos. Gli utenti possono accedere ad app non Elastos utilizzando il proprio ID Elastos Smart Web. Gli utenti possono inoltre salvare i propri dati delle app non di Elastos nel relativo spazio cloud di Elastos.
- Entrambi gli smart contracts Elastos e le app decentralizzate di Elastos (Dapps) funzionano sull' Elastos Smart Web. Questo crea una piattaforma chiusa ed evita la necessità di muoversi dentro e fuori la blockchain. Questa piattaforma chiusa crea una zona economica speciale in cui gli utenti possono sentirsi al sicuro mentre scambiano le risorse digitali. Ciò consente l'instauramento di un ciclo chiuso di produzione, transazione e consumo che è necessario per creare valore.

Di seguito vengono elencati alcuni dei benefici peculiari di Bitcoin, Ethereum e Elastos:

- Bitcoin = Libro mastro affidabile
- Ethereum = Libro mastro affidabile + Smart contracts
- Elastos = Libro mastro affidabile + Smart contracts + DAPPS Monetizzabili e Beni Digitali

La tecnologia blockchain esistente permette la registrazione dei diritti di proprietà. Sebbene gli utenti possano confermare che un libro digitale appartenga a loro, non possono invece prevenire che terzi siano in grado di leggere o rubare i libri senza autorizzazione. In queste condizioni è molto difficile monetizzare i beni digitali. Elastos mira a risolvere questo problema creando un ambiente nel quale l'esecuzione di un bene digitale (per esempio la visione e/o compravendita di un film) si effettua nel Web Intelligente di Elastos, e di conseguenza risponde alle regole degli Smart contracts. Il creatore di contenuti digitali può utilizzare uno strumento, fornitogli da Elastos, per

definire la quantità di contenuti digitali da creare. Gli autori, per esempio, posso decidere di avere solo 5000 copie disponibili dei loro libri nello Smart Web. Impostare una quantità limitata di contenuti digitali produce scarsità, permettendo la creazione di valore. Elastos punta inoltre a permettere agli consumatori di diventare investitori. Prendiamo in considerazione che ci siano 5000 libri digitali in circolazione e che diventino estremamente popolari. Ciò significa che ciascuno di questi libri aumenterebbe di valore, creando un potenziale guadagno per le persone che lo avevano comprato. Dopo aver letto e apprezzato il libro, il consumatore può decidere di rivenderlo a qualcun altro ad un prezzo maggiorato. Gli utenti possono comprare anche giochi in edizione limitata e, dopo averne fruito grazie all'Elastos Runtime nel loro smartphone, possono decidere di rivenderli ad altre persone. Il fatto che questi giochi siano ad edizione limitata, il loro valore nel mercato di seconda mano può variare.

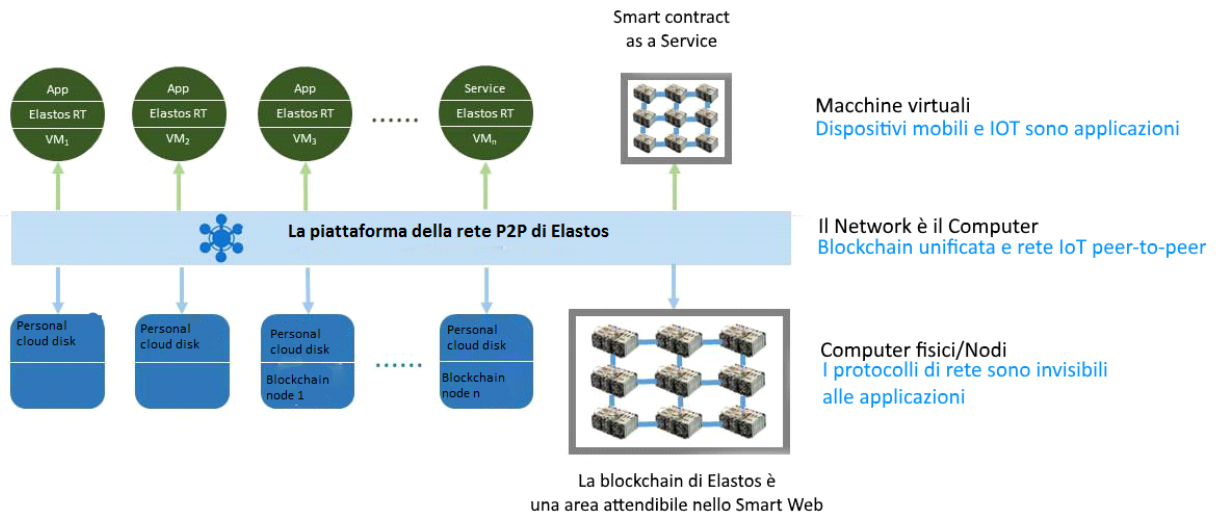
In un altro ambito di applicazione, i cineasti sarebbero in grado di raccogliere fondi per i loro film attraverso il finanziamento collettivo emettendo i loro token. I cineasti potrebbero scrivere uno smart contract stabilendo che ogni volta che qualcuno guarda il film i possessori di token ricevano una piccola quota dei guadagni. I registi potrebbero anche scrivere un differente smart contract per permettere agli spettatori di vendere il film peer-to-peer o via social network e percepire guadagni.

Questo sistema crea opportunità finanziarie sia per i creatori sia per i consumatori, incentivando così più persone a utilizzare Elastos. L'incremento di utenti incentiverà più creatori di contenuti digitali a produrre e pubblicare contenuti sulla piattaforma Elastos. Questo incremento di contenuti potrebbe quindi attirare ancora più utenti che, a loro volta, creeranno ulteriori contenuti. Questo è quindi un circolo virtuoso che può tradursi in una grande quantità di contenuti digitali di valore che può essere utilizzato per generare utile.

4. Piattaforma di Smart Web decentralizzato

Il grafico seguente illustra le relazioni tra i componenti chiave della piattaforma Elastos:

Costruzione di una piattaforma Smart Web Decentralizzata



4.1 Diritto di autenticazione degli Asset Digitali, Trading e circolazione

Il concetto di scarsità dell'età agricola è stato sostituito dai Big Data nell'era dell'informazione. Oggigiorno, le risorse digitali possono essere duplicate senza costi. Anche se i beni digitali sono ampiamente prodotti, diffusi e fruiti, non necessariamente creano valore. Quando le risorse digitali non sono autenticate, questo porta a effetti collaterali come la pirateria o la mancanza di motivazione necessaria alla creazione di innovazioni originali. La tecnologia blockchain affronta questo problema rendendo le risorse digitali autenticate e scarse. Elastos fornisce l'infrastruttura per l'autenticazione, il commercio e la circolazione di beni digitali. Quando qualsiasi tipo di risorsa digitale viene pubblicata online attraverso la blockchain, essa avrà la propria autorizzazione e in seguito questa risorsa potrà essere scambiata o commercializzata.

Il portafoglio di Elastos deve essere usato per pubblicare una risorsa digitale ed il saldo dovrebbe essere sufficiente per pagare la commissione al *miner*. L'editore di una risorsa digitale può creare richieste di autenticazione, che includeranno informazioni come l'indirizzo del portafoglio utente, l'URI (Uniform Resource Identifier), il prezzo e la quantità disponibile della risorsa stessa. Successivamente, il codice hash verrà elaborato e la transazione verrà registrata sulla catena come un output di transazione non speso (UTXO). Quando la registrazione dell'autenticazione delle risorse è pubblicata sulla blockchain, essa diventerà una risorsa digitale fruibile e negoziabile. Dopo aver

acquistato la risorsa, la proprietà del bene digitale acquistato viene trasferita al cliente, consentendo un'eventuale futura vendita.

4.2 Applicazioni decentralizzate (Dapps)

Se ci si basa sulla attuale sistema blockchain e delle criptovalute, finora non ci sono Dapp che possano competere con le applicazioni tradizionali. La ragione è che la potenza di calcolo e le operazioni di input / output al secondo (IOPS) delle Dapps sono relativamente scarse. L'attuale infrastruttura blockchain può essere facilmente messa in crisi. Elastos presenta un nuovo paradigma di calcolo e consentirà alle applicazioni decentralizzate di operare con un IOPS equivalente alle applicazioni tradizionali.

La blockchain di Elastos è progettata per usare una catena principale e varie catene secondarie. Per evitare di sovraccaricare la catena principale con dati non necessari, tutti gli smart contracts e le applicazioni verranno eseguiti sulle catene secondarie. Gli utenti possono facilmente sviluppare Dapp sicure ed avviarle da dispositivi hardware basati sul sistema operativo Elastos. Altrimenti, le dapp possono utilizzare l'ambiente Elastos Runtime su sistemi operativi tradizionali (Android, iOS, Windows, ecc.) per sviluppare applicazioni decentralizzate. Elastos Runtime può essere accessibile tramite VM e SDK.

5 La Blockchain di Elastos

In modo simile al sistema operativo su dispositivo mobile, gli utenti hanno bisogno di uno spazio affidabile per archiviare dati importanti. La blockchain di Elastos funge da zona attendibile per l'intero sistema operativo di rete.

La blockchain di Elastos sfrutta soluzioni basate su catena principale/secondarie per facilitare i processi della smart economy e per creare un fiorente sistema di applicazioni decentralizzate. Ciò significa che ogni applicazione può creare le proprie catene secondarie. La blockchain di Elastos fornisce supporto integrato per catene secondarie, completo e di facile implementazione. Le catene secondarie saranno inoltre personalizzabili, permettendo ai clienti di scegliere un metodo di consenso diverso a seconda dei caso d'uso.

L'emissione di token può avvenire direttamente sulle catene secondarie. Questi token possono partecipare a trasferimenti di risorse bidirezionali tra le catene principali e secondarie. Allo stesso tempo, grazie al *merged mining*, il consumo di energia sarà ridotto al minimo evitando elevati costi di elettrici ed evitando l'impatto ambientale legato alle emissioni di carbonio.

5.1 Commercio e struttura dei Blocchi

La struttura della blockchain di Elastos si basa sui sistemi di criptovaluta esistenti introdotti per la prima volta da Bitcoin. Quest'ultima include requisiti per la verifica dei blocchi come l'hash del blocco precedente, l'hash del Merkle tree, un *nonce* per l'algoritmo del consenso, la marcatura temporale (*timestamp*), il sistema di calcolo della difficoltà ed altro ancora.

Elastos migliora l'attuale esperienza delle valute digitali ed adotta una filosofia di progettazione delle sidechains. Elastos può adottare funzionalità che migliorano le sidechains come la rimozione degli script di convalida dalla struttura delle transazioni. La sidechain è la base per l'esecuzione di Dapps su Elastos, mentre la struttura della catena principale fornisce l'infrastruttura ed il supporto sulla quale edificare le sidechains, consentendo un adeguato trasferimento dei beni digitali.

5.2 Estrazione combinata (Merged Mining)

La blockchain di Elastos si avvale del mining combinato con Bitcoin, processo secondo al quale viene raggiunto il consenso su entrambe le catene contemporaneamente. In questo caso, la blockchain Bitcoin funziona come blockchain principale per Elastos, con la catena Elastos come blockchain ausiliaria. Le *mining pools* forniranno il codice per il merged mining e i minatori invieranno la Proof of Work (PoW) ad entrambe le blockchain in contemporanea. Il consumo d'energia non aumenta con l'estrazione combinata rimanendo uguale all'energia impiegata per l'estrazione di ognuna di esse. Attraverso questo meccanismo, la blockchain di Elastos garantisce elevatissime potenze di calcolo e sarà quindi in grado di fornire innovazioni nel settore blockchain su scala globale, facendo pieno uso delle esistenti risorse di calcolo dedicate al Bitcoin, con il valore aggiunto offerto dalla pocanzi menzionata sostenibilità ambientale. Ulteriori vantaggi dell'estrazione combinata includono:

- Il trasferimento della fiducia su più catene. La catena principale di Elastos viene minata insieme alla catena principale di Bitcoin. Questa modalità può essere estesa alle sidechains di Elastos, a patto che le sidechains adottino lo stesso meccanismo di consenso basato sulla PoW. Quindi, i vari livelli di blockchains (*layers*) possono essere co-minati in modo ricorsivo, il che stabilisce una struttura gerarchica di fiducia tra le varie catene.
- Nodi isolati. Una blockchain ausiliaria, o sidechain, dipendente dal merged mining non richiede un consenso distribuito su più nodi. In uno scenario estremo, una catena ha bisogno di un solo nodo e questo non diminuisce l'affidabilità delle informazioni contenute nel *ledger* sulla catena principale o in altre. Nessun altro algoritmo di consenso su blockchain ha questo tipo di vantaggio.

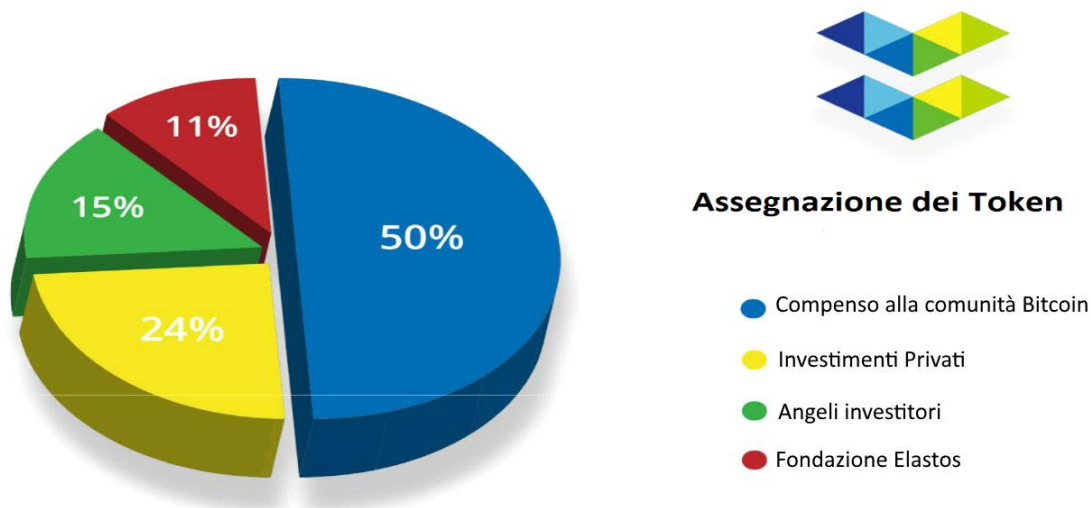
5.3 Piano di distribuzione dei token

Il token di Elastos, o ELA, è il token specifico della blockchain di Elastos e può essere utilizzato per il trading, per investire in beni digitali, per pagare le commissioni di elaborazione sulla blockchain, e così via. ELA è l'unità di base, inoltre, in onore del fondatore delle criptovalute Satoshi Nakamoto, Elastos vorrebbe utilizzare il Satoshi ELA (Sela) come minima frazione di ELA. 1 ELA equivale a 10^8 Sela, corrispondente alla centomillesima parte.

Elastos emetterà una quantità limitata di token. Il numero totale di Bitcoin raggiungerà infine i 21 milioni, mentre Elastos vorrebbe creare un totale di 33 milioni di ELA. Il piano di distribuzione ELA e le procedure di implementazione sono le seguenti:

ELA (unità:10000) 1650 (50%)	Scopo Sviluppo dell' ecosistema	Appunti Basandosi sul momento in cui viene creato il genesis block (il primo blocco) di Elastos, Elastos considererà i possessori di Bitcoin e potrebbe inviargli ELA gratuitamente. Nel dettaglio, le regole sono le seguenti: <ul style="list-style-type: none">• Target: feedback alla comunità delle criptovalute e creazione di una buona quantità circolante-• Quantità: i possessori di Bitcoin possono ottenere l'importo equivalente in ELA• Canale: distribuzione di ELA solo tramite exchanges di criptovalute autorizzati• Metodo: la Fondazione Elastos autorizzerà gli
---------------------------------	------------------------------------	--

		<p>exchanges ad emettere token, nessuno otterrà automaticamente ELA</p> <ul style="list-style-type: none"> • Tutti gli ELA non rivendicati verranno investiti in Elastos e non saranno utilizzati per le operazioni giornaliere della Fondazione Elastos
500(15%)	Angeli investitori (investitori informali)	Gli angeli investitori di Elastos sono costituiti dai fondatori di Elastos e da partner chiave. Il ricavo in Bitcoin andrà alla Fondazione Elastos
800(24%)	Raccolta fondi privata e pubblica	La comunità degli investitori è la spina dorsale di Elastos, supporterà e faciliterà lo sviluppo di Elastos. Tutta la criptovaluta raccolta apparterrà alla Fondazione e sarà usata per sviluppare la piattaforma. I ricavi in Bitcoin andranno alla Fondazione Elastos
350(11%)	Fondazione di Elastos	Questi fondi sono pre-assegnati per supportare le operazioni della fondazione di Elastos ed investire nell'ecosistema Elastos



Per far fronte alla perdita naturale di token, causata ad esempio dagli utenti che perdono l'accesso ai loro wallet, oltre che per garantire una leggera inflazione, il numero di ELA in circolazione aumenterà ogni anno ad un tasso fisso del 4%.

Gli ELA verranno prodotti ogni due minuti durante il merged mining con Bitcoin. Queste nuove monete coniate saranno assegnate alla Fondazione Elastos e ai minatori. La Fondazione Elastos prenderà il 30%, il restante 70% appartiene ai minatori.

5.4 Catene Laterali - Sidechains

Qualsiasi sistema costruito con tecnologia blockchain ha meno potenza di calcolo rispetto a un computer tradizionale, per questo motivo esso non sarà in grado di soddisfare i vari requisiti delle applicazioni che sfruttano Internet (come videogiochi o lo streaming di film in alta definizione). Questo è fondamentalmente il motivo per cui la tecnologia blockchain non può ancora essere applicata su larga scala in Internet. Il team di Elastos riconosce questo aspetto e pertanto ritiene che lo sviluppo di blockchain dedicate al calcolo non debba affidarsi esclusivamente ad una catena principale. Elastos punta a scalare il sistema di blockchain fornendo il supporto alle catene laterali (sidechains), le quali aiuteranno a soddisfare i requisiti per l'esecuzione di applicazioni con IOPS elevati.

La catena principale di Elastos sarà responsabile del piccolo ma molto importante ruolo

nello scambio e trasferimento di ELA, fornendo così stabilità al sistema blockchain. Elastos vuole evitare di sovraccaricare la catena principale con smart contracts non necessari, quindi solo i principali aggiornamenti infrastrutturali si svolgeranno sulla catena principale. Tutti gli altri smart contracts possono essere implementati su catene laterali, consentendone la scalabilità.

Questo tipo di filosofia di progettazione gerarchica e strutturata aprirà la strada a un futuro paradigma di blockchain, come il già citato progresso da un calcolo autonomo a uno distribuito. Questa è un'innovazione chiave nella tecnologia blockchain, più importante della tecnologia limitata di algoritmi e catene a consenso unico.

Il team implementerà servizi di base come sidechain per uso pubblico e globale. Questi servizi includono la generazione di ID, la distribuzione di token, il trading di beni digitali e i sistemi di pagamento rapido. Questi servizi di base, tutti importanti componenti infrastrutturali, fanno parte dello Smart Web di Elastos. In aggiunta, il team fornirà anche supporto per lo sviluppo di sidechain di terze parti.

Le transazioni sono la parte più importante dell'interfaccia tra le catene principali e laterali. La procedura di transazione per l'invio di token dalla catena principale a una sidechain equivale all'invio da un account utente sulla catena principale a un indirizzo a firma multipla corrispondente al sidechain. Il processo verifica automaticamente che la sidechain possa identificare la transazione e depositare il valore equivalente dei token sull'account nella sidechain.

Procedura di transazione da catena principale a sidechain:

- L'utente crea un codice segreto casuale e il suo hash corrispondente.
- L'utente costruisce un indirizzo di firma multipla sulla catena principale. Per sbloccare la transazione, devono essere forniti sia il codice segreto che la chiave privata dell'utente dell'indirizzo di firma multipla.
- L'utente invia la transazione e l'hash del proprio codice segreto al nodo di elaborazione delle transazioni della sidechain.
- Il nodo di elaborazione delle transazioni sulla sidechain genera la transazione in uscita dopo l'autenticazione mediante hash e chiave privata a firma multipla.
- L'utente fornisce il codice segreto per sbloccare la transazione e ricevere i token dalla sidechain.

- I token vengono depositati sull'indirizzo a firma multipla.

La procedura di transazione per l'invio di ELA da sidechain a catena principale equivale all'invio di ELA da un indirizzo a firma multipla sulla catena principale ad un account utente che si trova sulla catena principale.

Procedura per la transazione da catena laterale a catena principale:

- L'utente crea un codice segreto casuale e il suo hash corrispondente.
- L'utente crea una transazione sulla sidechain sbloccabile unicamente fornendo il codice segreto.
- L'utente invia la transazione e l'hash del codice segreto ai nodi di elaborazione delle transazioni della catena principale.
- Il nodo di elaborazione della transazione sulla catena principale genera la transazione in uscita dopo l'autenticazione mediante hash e chiave privata a firma multipla.
- L'utente fornisce il codice segreto per sbloccare la transazione ricevendo i token dalla catena principale.
- L'indirizzo di firma multipla corrispondente alla catena laterale sblocca il ritiro e spende i relativi token.

Per controllare la sicurezza di ELA su un indirizzo a firma multipla, l'indirizzo può generare come descritto in precedenza solo una transazione di prelievo di token.

5.5 Smart Contracts

Se sulla catena principale vengono implementati gli smart contracts computazionalmente impegnativi, anche nel caso in cui non vengano invocati, è comunque necessario aggiornare costantemente ogni nodo della rete. Questo è un onere per i nodi di verifica puri in quanto i nodi di mining possono ancora ricevere le commissioni per l'elaborazione delle transazioni. Per evitare ciò, la catena principale di Elastos limita l'utilizzo degli smart contracts e li delega alle sidechains. Ogni sidechain è in grado di gestire autonomamente la funzionalità dello smart contract, in modo simile a come NeoContract supporta la blockchain NEO.

6. Elastos carrier: una rete P2P decentralizzata

L'Elastos carrier è il servizio Internet decentralizzato offerto dall'ecosistema di Elastos. I suoi nodi possono essere eseguiti all'interno di qualsiasi ambiente connesso a Internet, comprese le reti locali all'interno di una casa o di un luogo di lavoro. Utilizzando tecniche di trasparenza NAT (User Datagram Protocol, Network Address Translator) basate su UDP, tutte le coppie di nodi avranno il potere di stabilire connessioni tra loro, anche con connessioni dirette. Ciò consentirà un esteso utilizzo delle capacità individuali di ogni nodo, il che servirà ad aumentare l'efficacia della potenza di calcolo della rete nel suo complesso.

L'insieme dei servizi di base includerà nomi di dominio decentralizzati, il calcolo decentralizzato e l'archiviazione decentralizzata. Verrà incluso il supporto per lo sviluppo di Dapps. All'interno di tale ambiente, l'utente può possedere i propri dati e calcoli con un livello significativo di protezione della privacy. Allo stesso tempo l'utente avrà il potere di affittare a proprio piacimento la propria attrezzatura tramite Elastos Blockchain, potrà quindi percepire una remunerazione in base alla quantità di calcolo e di spazio di archiviazione consumato, motivando lo sviluppo di un mercato basato su Elastos.

7. Sistema operativo Elastos: un sistema operativo sicuro e di ampia fruibilità

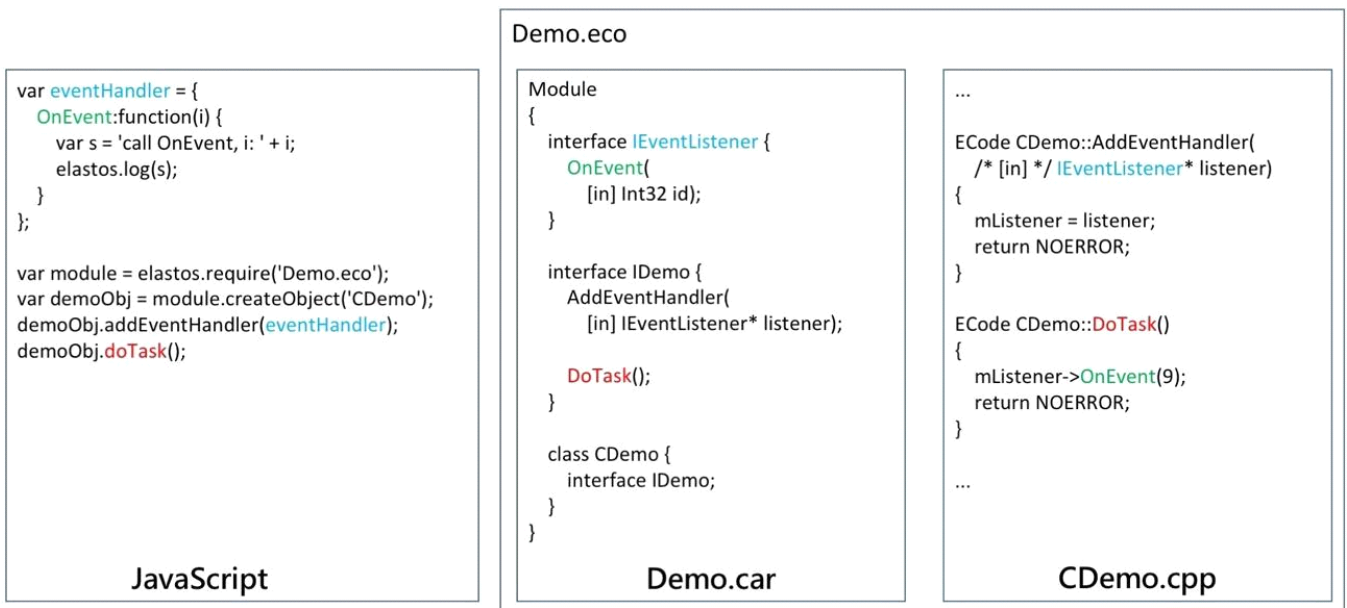
Elastos OS è un sistema operativo ad ampio margine di utilizzo basato sul rispetto per la sicurezza. È un sistema operativo fatto per soddisfare le esigenze dell'Internet of Things (IoT), di *invention kit* come il Raspberry Pi e di dispositivi mobili. L'ultima versione, la terza, è stata sottoposta a un processo di mercificazione dal maggio 2013, ha raggiunto con successo la versione beta, essendo stata testata e analizzata sul telefono Moto X (XT1085) e sullo smart router Lamobo-R1S. La quantità totale di stringhe codice ha superato i 10 milioni di linee.

Per quanto riguarda la sicurezza, Elastos OS vieta la creazione diretta dei processi e non consente l'interazione diretta con TCP/IP, dipendendo invece dal sistema per generare automaticamente e determinare la posizione dei microservizi locali, prossimi e distanti (o basati su cloud). Il sistema genererà automaticamente Remote Procedure Calls (RPC) e fornirà risposte basate su eventi, evitando così possibili azioni malevole da parte dell'applicazione o del servizio remoto, opponendosi inoltre all'ulteriore diffusione dei virus.

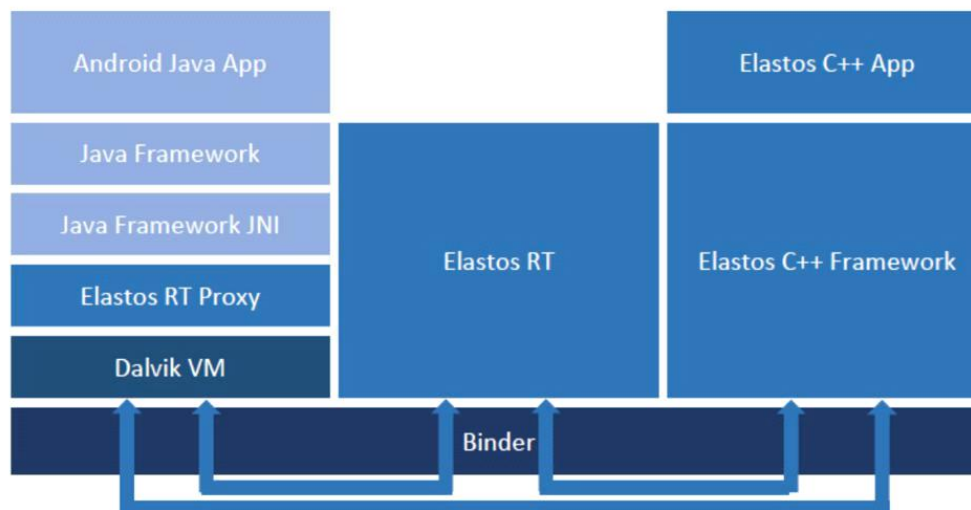
Elastos OS fornisce un sistema di supporto decentralizzato intrinseco e migliorato per le applicazioni in fase di sviluppo, facilitando l'interfacciamento con Elastos Carrier per

l'ottenimento dei servizi di base e per interfacciarsi con Elastos Chain per ottenere servizi relativi al credito e allo scambio. Le Dapp risultanti possono tranquillamente e contemporaneamente gestire le transazioni Elastos e altri tipi di beni digitali, tra cui: codice sorgente, dati, libri elettronici, video e articoli da gioco. Potrebbero gestire tra le altre cose il copyrigt, le transazioni e la circolazione.

Il sistema utilizzerà C/C ++, Java e HTML5/JS come modalità di sviluppo principali. La sua API C++ rispecchierà in gran parte le API Java di Android, consentendo la gestione unificata "tre in uno" dell'accesso al cloud, del monitoraggio e dell'interfaccia. I componenti scritti in Java, HTML5/JS e C/C++ saranno in grado di richiamarsi e comunicare con l'un l'altro in modo modulare, senza la necessità di gestire manualmente il JNI. In quanto tale, il sistema è conforme alla massima di "scrivi una volta, esegui ovunque". Il sistema supporterà l'architettura Component Assembly Runtime (CAR), come dimostrato dall'esempio seguente, che utilizza un componente CAR per stabilire la comunicazione tra un programma scritto in C/ C++ e uno in HTML5/JS.



Il framework C++ di Elastos OS, utilizzando le interfacce applicative di Android, garantisce allo sviluppatore sia praticità che portabilità. Elastos OS si spinge fino al punto di eseguire direttamente i programmi Android, raggiungendo così la seguente situazione:



Si può pensare a Elastos Runtime come alla versione C++ della Java Virtual Machine così come al framework Java. Ci si può riferire ad esso anche come C Virtual Machine (CVM). I servizi e le applicazioni del sistema operativo Elastos saranno eseguiti all'interno di questo CVM, consentendo ai servizi stessi l'esistenza in armonia con un panorama variegato di nodi e piattaforme hardware.

8. L'Ambiente Elastos Runtime per le DAPPs

Sebbene Elastos OS possa essere eseguito in qualsiasi momento al fine di godere del supporto completo e primario per lo sviluppo di Dapps, ci sono altre numerose occasioni in cui l'utente potrebbe preferire un altro sistema operativo già disponibile. In questi casi, è possibile utilizzare Elastos Runtime: un ambiente di runtime che offre parimenti supporto completo per le applicazioni in questione. Gli sviluppatori potranno scegliere tra Elastos Runtime per Android, Elastos Runtime per iOS ed Elastos Runtime per Ubuntu Linux, a seconda delle loro esigenze.

8.1 Interfaccia di rete P2P

Non avendo la possibilità di connettersi direttamente ad internet le Dapp devono comunicare tra loro tramite interfacce a componenti. Questo approccio è più facile, più sicuro e più naturale:

```

5
6 TrustID myfriend = "0xE94b04a0FeD112f3664e45adb2B8915693dD5FF3";
7 IChat * pChat = CChat::New(myfriend);
8 pChat->Chat("hello");
9

```

Il codice sopra riportato non ha bisogno di considerare la serializzazione/deserializzazione o crittazione/decrittazione, né il programmatore necessita di essere coinvolto nella scrittura di nuovi protocolli. Tutte queste cose possono essere soddisfatte dall'interfaccia CAR di Elastos Runtime. Tutto ciò che si deve fare è modificare il documento CAR di seguito, quindi produrre le funzioni corrispondenti. Ne consegue che rispetto alla consueta API basata sui socket, Elastos Runtime è molto più facile da usare. Inoltre, si può eseguire una transazione di beni digitali come visto di seguito:

```

13
14 interface IChat {
15     Chat(String message);
16 }
17
18 class CChat {
19     interface IChat;
20 }
21

```

Il codice seguente mostra come effettuare transazioni:

```

24
25 ECode CChat::Chat(String message) {
26     // your code ....
27
28     return NOERROR;
29 }
30
31

```

Le applicazioni scritte utilizzando Elastos Runtime sono più semplici delle applicazioni di rete P2P scritte utilizzando l'API socket tradizionale.

8.2 Operazioni sulle risorse digitali

Come mostrato negli esempi precedenti per le comunicazioni di rete non usiamo più indirizzi IP o nomi di dominio perché Internet attuale non è affidabile. Tuttavia, Elastos Runtime eseguirà la verifica del runtime durante lo sviluppo di Elastos Runtime con la trust zone, vale a dire la Elastos Blockchain appunto.

```

33
34 ECode _CChat::Chat(String message) {
35     ... ..
36     ... ..
37     // Check whether ID is exist
38     if (Exist(trustID) == FALSE) {
39         return ERROR;
40     }
41     // Check whether the current APP ID is on the blacklist
42     if (InBlackList(_Current_App_TrustID) == TRUE) {
43         return ERROR;
44     }
45     // Check whether the current user ID is on the blacklist
46     if (InBlackList(_Current_User_TrustID) == TRUE) {
47         return ERROR;
48     }
49     // Check whether the called count has exceeded the upper limit
50     if (Called_Count > MAX_CALL_COUNT) {
51         return ERROR;
52     }
53     }
54     // More checks
55     ... ..
56     ec = CChat::Chat(message);
57     ... ..
58     return ec;
59 }
60
61
62
63
64

```

In questo modo le transazioni di beni digitali possono essere eseguite. Il seguente esempio verifica la proprietà delle risorse digitali:

```

66
67 TrustID aMovie = "0x32B77CBB265175D1A927c9A3F816de577BDDdE05";
68 TrustID owner = "0xd4fa1460F537bb9085d22C7bcCB5DD450Ef28e3a";
69
70
71 if (Elastos.RT.Trust.CheckOwner(owner, aMovie) == TRUE) {
72     // yes, He is its owner.
73 }
74 else {
75     // error
76 }
77
--

```

Infine, viene creata e inviata una transazione:

9. La Fondazione Elastos

Il progetto Elastos ha una lunga storia. Il suo precursore risale al 2000, quando il fondatore Rong Chen tornò in Cina per iniziare la sua attività. Da allora, Rong Chen si è dedicato allo sviluppo di un sistema operativo sicuro e generico per l'era di Internet. Nel 2017, il progetto Elastos è diventato un progetto di software open source globale e gratuito guidato dalla comunità di Elastos. Il codice sorgente dei documenti software sviluppati è pubblicato con licenza software gratuita ed open-source. Il progetto Elastos è gestito attraverso la Fondazione Elastos abbracciando la libera comunità open source e la moneta digitale e supportando l'apprendimento reciproco promuovendo il progresso della civiltà umana.

9.1 La Comunità Elastos

La community globale di Elastos include fan, sviluppatori, organizzatori di comunità e titolari di token Elastos in tutto il mondo. Elastos è impegnata a estendere ulteriormente questa comunità globale. Elastos ha anche in tutto il mondo una comunità di gruppi di utenti locali che lavorano per la comunità come volontari. Questi gruppi di utenti organizzano, mantengono e sviluppano le comunità locali di Elastos. I loro compiti includono la promozione delle valute digitali e la filosofia blockchain, lo studio della tecnologia Elastos, la partecipazione allo sviluppo del progetto Elastos, la stesura e traduzione di documenti, l'organizzazione di incontri mensili locali e l'organizzazione di attività globali ufficiali di Elastos.

9.2 Talenti di Elastos

Siamo ancora nelle prime fasi della valuta digitale e della blockchain. Il settore si sta rapidamente sviluppando e c'è carenza di talenti. I fondatori di Elastos hanno avviato il programma "We are all Satoshi Nakamoto (Siamo tutti Satoshi Nakamoto)" presso il Tsinghua iCenter attraverso la Distributed Autonomous Coalition Asia (DACA), che mira a coltivare talenti tecnologici in blockchain di alto livello. Dalla sua implementazione, questo programma ha coltivato una grande quantità di talenti nel settore, alcuni dei quali gradualmente sono diventati pilastri del team Elastos. La Fondazione Elastos supporterà continuamente i progetti di formazione DACA e collaborerà con Tsinghua iCenter per lo sviluppo tecnologico della comunità cinese della blockchain.

9.3 La visione di Elastos

Elastos sta lavorando per diventare la tecnologia che alimenta la smart economy. Il Fondo di Elastos investirà nello sviluppo continuo di applicazioni decentralizzate nell'intenzione di creare un nuovo World Wide Web che sia più sicuro, più intelligente e che un giorno possa essere conosciuto come Internet del Valore.