CyberMiles: un protocollo di blockchain di prossima generazione per le transazioni commerciali

Di 5xlab

Un whitepaper tecnico

v1.5

[Gli scenari commerciali e i termini di vendita dei token sono discussi in un documento separato]

Disclaimer

Questo è un documento concettuale ("Whitepaper tecnico") che descrive il nostro protocollo e la direzione della blockchain CyberMiles per lo sviluppo della sua rete. Può essere modificato o sostituito in qualsiasi momento. Tuttavia, non vi è alcun obbligo di aggiornamento per il Whitepaper tecnico o nel fornire al destinatario l'accesso a qualsiasi informazione aggiuntiva.

I lettori vengono avvisati per come segue:

Non disponibile per tutte le persone: la piattaforma CyberMiles e i token CyberMiles non sono disponibili per tutte le persone. La partecipazione può essere soggetta a una serie di passaggi, inclusa la necessità di fornire determinate informazioni e documenti.

Nessuna offerta di prodotti regolamentati in alcuna giurisdizione: i token CyberMiles (come descritto in questo documento tecnico) non intendono costituire titoli o altri prodotti regolamentati in alcuna giurisdizione. Questo Whitepaper tecnico non costituisce un prospetto né offre documenti di alcun tipo e non intende costituire un'offerta o una sollecitazione di titoli o prodotti regolamentati in alcuna giurisdizione. Questo whitepaper tecnico non è stato esaminato da alcuna autorità di regolamentazione di qualsiasi giurisdizione.

Nessun consiglio: questo Whitepaper tecnico non costituisce un consiglio in merito alla partecipazione o meno alla piattaforma CyberMiles o all'acquisto di token CyberMiles, né deve essere invocato in relazione a qualsiasi contratto o decisione di acquisto.

Nessuna dichiarazione o garanzia: Nessuna dichiarazione o garanzia viene fatta in merito all'accuratezza o alla completezza delle informazioni, dichiarazioni, opinioni o altre questioni descritte in questo documento o altrimenti comunicate in connessione con il progetto. Senza limitazioni, non viene fornita alcuna dichiarazione o garanzia in merito al raggiungimento o alla ragionevolezza di dichiarazioni previsionali o concettuali. Nulla in questo documento è o dovrebbe essere invocato come una promessa o una rappresentazione per il futuro.

Nella misura massima consentita dalla legge applicabile, qualsiasi responsabilità per qualsiasi perdita o danno di qualsiasi natura (prevedibile o meno) derivante da o in relazione a qualsiasi persona che agisca in questo WhitePaper tecnico, o qualsiasi aspetto di esso, nonostante qualsiasi negligenza, inadempienza o mancanza di cura, è declinato. Nella misura in cui la responsabilità può essere limitata ma non completamente rifiutata, è limitata nella misura massima consentita dalla legge applicabile.

Altre società: diverse da CyberMiles Foundation Limited **("Foundation"**) e 5miles LLC **("5miles"**), l'uso di qualsiasi nome e marchio di società e / o piattaforma non implica alcuna affiliazione o approvazione da parte di tali soggetti . I riferimenti in questo whitepaper tecnico a società e piattaforme specifiche sono solo a scopo illustrativo.

È necessario prendere tutta la consulenza professionale necessaria, anche in relazione al trattamento fiscale e contabile. Speriamo che il progetto CyberMiles abbia un grande successo. Tuttavia, il successo non è garantito e le risorse e le piattaforme digitali comportano rischi. Devi valutare i rischi e la tua capacità di sopportarli.

Sintesi

La tecnologia blockchain è molto promettente per le applicazioni aziendali. Tuttavia, le blockchain di generazione attuale soffrono di bassa efficienza di esecuzione e bassa produttività degli sviluppatori. Di conseguenza, non sono ampiamente adottati per le transazioni commerciali comuni. In questo documento, presentiamo un nuovo protocollo di rete blockchain, chiamato blockchain CyberMiles, che è specificamente ottimizzato per le transazioni dei contratti commerciali.

La nostra soluzione proposta è un'innovazione del protocollo che rende accessibile una serie di tecnologie middleware* a una macchina virtuale distribuita sulla blockchain. La nuova blockchain sarebbe altamente performante e scalabile supportando oltre 10.000 transazioni al secondo. Permetterà alle aziende di scrivere contratti aziendali intelligenti, che sono applicazioni middleware distribuite che codificano regole e processi aziendali. La valuta crittografica nativa della rete, il CyberMiles Token (CMT), può essere utilizzata per regolare le transazioni, premiare i validatori delle reti (che eseguono gli Smart Business Contracts) e incentivare i membri della comunità a fornirsi servizi a vicenda.

Un vantaggio unico della blockchain CyberMiles è che verrà implementato per supportare la rete di e-commerce "5Miles" già esistente di 5 milioni di oltre 10 milioni di utenti registrati negli Stati Uniti e oltre 3 miliardi di dollari in transazioni annuali stimate. Questo creerebbe immediatamente la più grande rete di commercio basata su blockchain nel mondo. La rete potrebbe fornire servizi quali l'identità utente decentralizzata e la gestione del credito, la stanza di compensazione dei regolamenti decentralizzati, il voto peer to peer basato sui pari e la risoluzione conflittuale. Esempi di applicazioni sulla piattaforma di rete includono "portafogli" decentralizzati di informazioni personali, prestiti alle piccole imprese peer-to-peer e arbitrati di controversie tra pari.

*Middleware: Insieme di software che fungono da intermediari fra strutture e programmi informatici, permettendo loro di comunicare a dispetto della diversità dei protocolli o dei sistemi operativi aziendali affidabili

Sommario

1. INTRODUZIONE

1.1 Bitcoin ed Ethereum

Il Bitcoin è la prima applicazione killer della tecnologia blockchain. La rete Bitcoin, nota come blockchain 1.0, è principalmente un sistema di registro distribuito con un meccanismo di consenso decentralizzato incorporato. Attraverso la tecnologia UTXO, sebbene sia possibile scrivere programmi da eseguire sulla rete Bitcoin, i programmi UTXO di basso livello hanno una capacità molto limitata. È un ambiente di programmazione incompleto, ed è molto difficile da usare. Di conseguenza, la rete Bitcoin è principalmente un sistema di registro distribuito per registrare transazioni bitcoin con pochissime applicazioni sviluppate dalla comunità.

Il progetto Ethereum mirava a costruire la Blockchain 2.0. Aggiungendo una macchina virtuale completa di Turing (chiamata Ethereum Virtual Machine, o EVM), la blockchain di Ethereum aspira ad essere il "computer del mondo" supportando script di terze parti noti come Smart Contracts per spostare token / criptovalute tra account quando vengono soddisfatte determinate condizioni (ad esempio, uno dei casi d'uso è che lo Smart Contract funga da account di garanzia). Questi Smart Contracts vengono eseguiti dai nodi Ethereum in tempo reale. I loro risultati sono convalidati e salvati nella blockchain da minatori “Miners” (o validatori). Inoltre, Ethereum supporta anche il concetto di app decentralizzate (alias DApps), che vengono eseguite al di fuori della blockchain ma possono effettuare chiamate ai metodi Smart Contract nella blockchain. In una configurazione tipica, un DApp potrebbe essere un'applicazione Web che fornisce un'interfaccia utente per il contratto intelligente corrispondente.

1.2 Problemi principali e lavoro correlato

Tuttavia, è anche ampiamente accettato che le tecnologie blockchain oggi soffrono dei problemi legati alla bassa efficienza e alla bassa produttività degli sviluppatori.

Come sistema decentralizzato, una rete blockchain richiede molti nodi indipendenti e non cooperativi per eseguire le stesse attività di elaborazione ripetutamente, e quindi raggiungere il consenso su ciò che è "vero". Ciò rende il sistema molto efficiente e difficile da scalare, poiché lo sforzo di elaborazione aumenta geometricamente con le dimensioni della rete. A causa del problema di scalabilità / prestazioni, le attività di computazione di terze parti consentite sulla rete blockchain devono essere anche molto limitate. Ciò, a sua volta, causa un'esperienza di sviluppo molto scarsa e una bassa produttività. Di conseguenza, le DApp di Ethereum Smart Contract non sono ampiamente utilizzate oggi.

Ci sono diverse soluzioni proposte all'orizzonte per affrontare i problemi di prestazioni e scalabilità della tecnologia blockchain.

• Nuovi meccanismi di consenso. Le blockchain di Bitcoin ed Ethereum utilizzano un meccanismo di consenso altamente efficiente chiamato Proof-of-Work (PoW) al fine di proteggere la rete da partecipanti non fidati. Molto lavoro è stato fatto per rimpizzare la POW con un più efficiente meccanismo chiamato Proof-of-Stake (PoS). I contendenti principali in questo spazio includono il motore di consenso alla tolleranza ai guasti bizantino "Bizantine fault tolerance "(BFT) di Tendermint, nonché la soluzione CASPER di Ethereum.

• Sharding of the network. Un approccio comune di utilizzo per scalare il network è suddividere una rete in diverse sottoreti. Quindi l'intera rete può scalare orizzontalmente aggiungendo altre sottoreti. In una rete di blockchain decentralizzata, tuttavia, le sub-reti devono comunicare tra loro e raggiungere il consenso sui loro stati. Questo è un problema molto più difficile rispetto al normale "sharding" del database. Le soluzioni principali in questo spazio includono "Cosmos Internet of Blockchains" e la rete "Polkadot".

• Calcoli fuori catena (Off Chains). Una soluzione ancora più diretta al problema delle prestazioni è spostare gran parte dei compiti di calcolo pesanti fuori dalla blockchain stessa e utilizzare il meccanismo di consenso blockchain per registrare solo i risultati computazionali. Ci sono anche molte sperimentazioni in questo spazio, che vanno dai canali di stato off-chain di Lightning Network, alle catene laterali antifrode di Plasma, al framework di transazione Ethereum Smart Contract di TrueBit fuori catena.

In questo articolo, non tenteremo di risolvere i problemi fondamentali della scalabilità della blockchain. Crediamo che, nel tempo, una buona soluzione emergerà dal consenso della comunità. Le future reti di blockchain incorporeranno tutti e tre gli approcci per diventare altamente performanti e scalabili.

Tuttavia, una volta risolti questi problemi, la rete blockchain deve ancora attirare e supportare gli sviluppatori di applicazioni aziendali per essere commercialmente utile. In questo progetto, il nostro obiettivo è proporre una soluzione architettonica per rendere le applicazioni aziendali di terze parti su reti blockchain (gli Smart Contracts) molto più potenti e molto più facili da sviluppare allo stesso tempo.

1.3 Un contratto intelligente migliore

Come tecnologia di prima generazione e per le ragioni di scalabilità / prestazioni di cui abbiamo discusso in precedenza, Ethereum EVM e DApp sono difficili da utilizzare. Miriamo a migliorare drasticamente l'EVM e il relativo stack software associato per renderlo più adatto agli sviluppatori e pronto per l'azienda.

• Lo Smart Contract deve spesso essere attivato da eventi esterni alla blockchain. In Ethereum, ciò richiede un "oracolo" per fornire informazioni di stato autorevoli e deterministiche del mondo esterno. L'oracolo è una soluzione fragile, in quanto non è standardizzata e potrebbe cambiare senza le conoscenze dello Smart Contract.

• Lo Smart Contract può essere solo liberamente associato alla middleware DApp. Senza "sapere" ciò che è disponibile in DApp, lo Smart Contract non può effettuare chiamate a nessun componente software della DApp. A causa della difficoltà computazionale di programmare regole complesse usando i linguaggi di programmazione procedurale completi di Turing, la maggior parte degli Smart Contracts implementa solo semplici regole di transazione commerciale.

• La DApp middleware non può essere incapsulato e riutilizzato. Gli sviluppatori DApp devono prendere decisioni architettoniche e scrivere applicazioni uniche.

• La DApp middleware non è integrato con il sistema di incentivi block-cryptovalute. I nodi DApp devono contribuire con una notevole quantità di risorse informatiche, ma non possono ricevere criptovaluta come ricompensa. Ciò ha comportato l'esecuzione centralizzata di DApps da parte delle società.

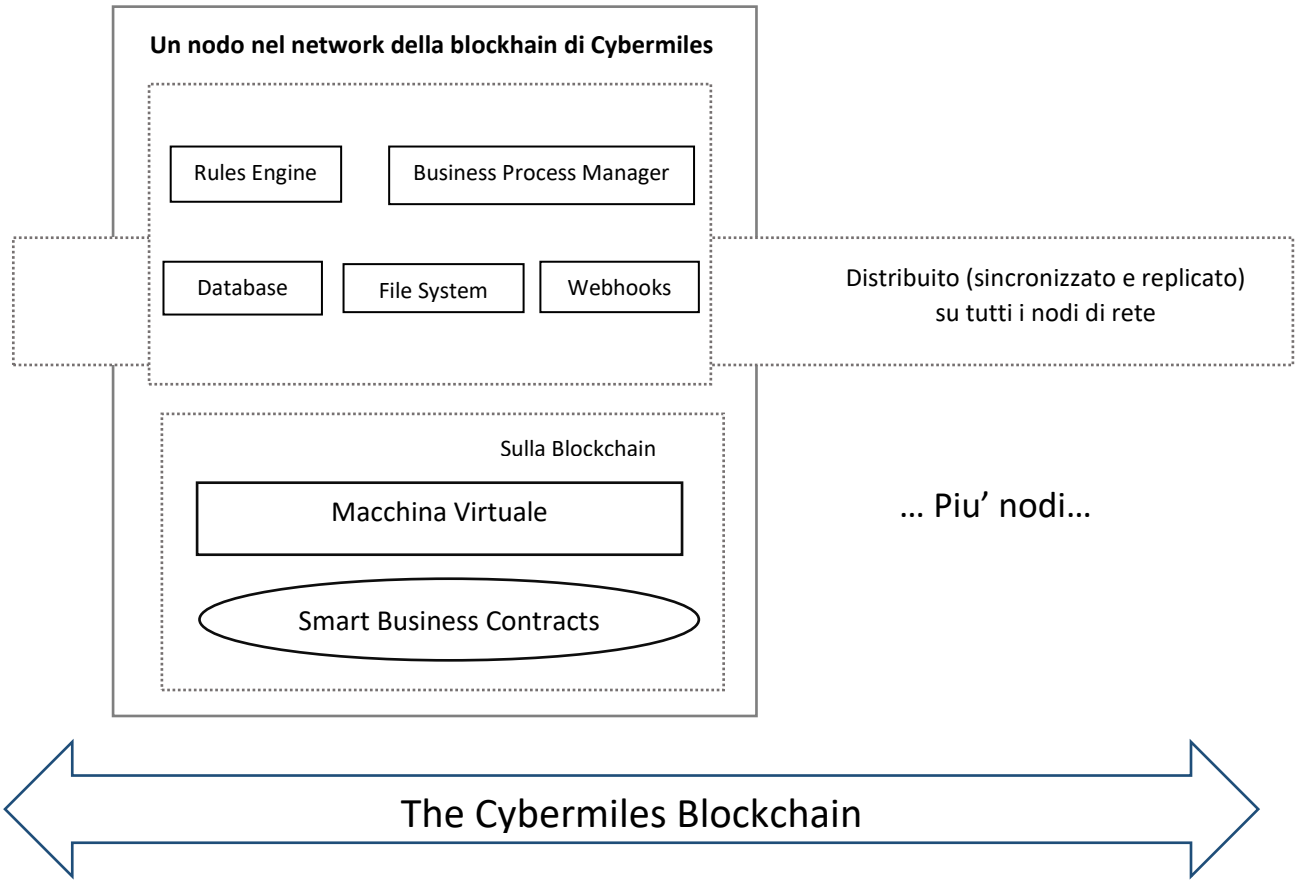
2. PROPOSTA SOLUZIONE

Per affrontare le carenze di Ethereum e creare una "macchina virtuale" basata su blockchain adatta agli sviluppatori di business per creare applicazioni distribuite, proponiamo un nuovo protocollo blockchain per supportare quello che definiamo "Smart Business Contract". Il protocollo non solo includerebbe una macchina virtuale, ma definirà anche lo stack del software middleware al di fuori della blockchain (che oggi è gestito da DApps in un modo non standard). Ogni nodo nella blockchain non solo eseguirà il blockchain ledger ma supporterà anche il middleware standardizzato.

Prendendo in prestito una pagina dal vecchio programma di successo del software aziendale, la chiave non è creare una totale macchina virtuale o un linguaggio di programmazione onnipotente,

ma costruire una vasta libreria di componenti software riutilizzabili e quindi standardizzare l'intera serie di software. Un buon esempio è il sistema operativo Linux. È ampiamente adottato dagli utenti aziendali solo dopo che la community ha esteso il sistema operativo principale con migliaia di pacchetti software business-friendly, e dopo che Fedora / Red Hat si sono uniti per standardizzare lo stack. Altri esempi precedenti includono la piattaforma Java (Java 2 Enterprise Edition plantform), o lo stack LAMP o anche la piattaforma Ruby on Rails. I punti di forza di queste piattaforme aziendali risiedono nelle loro librerie e framework standardizzati.

L'incapsulamento e il riutilizzo del software sono le best practice più importanti nei software per le imprese. È giunto il momento per noi di applicare questa best practice anche alla piattaforma blockchain.



La Figura 1. mostra l'architettura generale della blockchain CyberMiles. Come puoi vedere, una quantità significativa di componenti software riutilizzabili risiede al di fuori della blockchain.

2.1 Contratto Smart Business

Uno Smart Business Contract sulla blockchain di CyberMiles è analogo allo Smart Contract sulla blockchain di Ethereum. Viene eseguito dal nodo blockchain e convalidato dal miner quando viene creato un nuovo blocco.

I risultati dello Smart Business Contract vengono salvati nel nuovo blocco. Tuttavia, la differenza principale tra CyberMiles Smart Business Contract e Ethereum Smart Contract è che, invece di scrivere ogni applicazione da zero, uno Smart Business Contract avrebbe accesso a uno stack integrato e potente del software middleware aziendale. Pertanto, uno Smart Business Contract può essere facile da sviluppare e altamente riutilizzabile di per sé. Poiché lo Smart Business Contract fa parte della blockchain, la potenza di calcolo necessaria per eseguirla, compresi gli sforzi per eseguire l'intero stack di middleware aziendale esterno, possono essere considerati per utilizzare la criptovaluta del sistema CyberMiles, il CyberMiles Token (CMT).

Gli utenti della rete che effettuano transazioni pagano ai liquidatori di rete piccole commissioni di transazione in CMT per compensare il loro lavoro nel garantire l'integrità dei dati.

2.2 Lo Stack di middleware

Lo Smart Business Contract può accedere a framework di software aziendali al di fuori della blockchain stessa. Questi framework software sono incorporati in ognuno dei nodi che eseguono la blockchain. Tali quadri verranno eseguiti ogni volta che viene eseguito un Smart Contract

Business e quando i ministri blockchain convalidano i risultati. Lo stack di framework middleware enterprise incluso nel sistema CyberMiles include quanto segue.

• Un motore di regole. La maggior parte dei contratti commerciali deve seguire determinate regole. Rispetto ad un linguaggio di programmazione procedurale generico, è dimostrato che un motore di regole dedicato è facile da usare ed efficiente. È già utilizzato da molte aziende.

• Un business process manager (BPM). Un sistema BPM è una macchina a stati che imita lo stato di esecuzione di un contratto a più fasi. È guidato da azioni esterne da parti contraenti e il BMP in genere utilizza il motore delle regole per determinare i passaggi successivi.

• Un database distribuito. È necessario un database distribuito per supportare framework di applicazioni complessi e memorizzare i dati dell'applicazione. Questo database è replicato e sincronizzato attraverso i nodi sulla blockchain. Non memorizza i risultati delle transazioni, che verrebbero archiviati nella blockchain stessa.

• Un servizio distribuito di archiviazione di file e dati. Lo Smart Business Contract ei relativi servizi middleware dovranno accedere ai servizi di file per gestire file di dati più grandi richiesti per il processo decisionale.

• Un servizio webhook distribuito. Poiché un sistema aziendale deve interagire con entità esterne che completano gli obblighi contrattuali (ad esempio notifica di consegna FedEx per le applicazioni di e-commerce), costruiremo un sistema webhook distribuito in grado di ricevere eventi esterni relativi ai contratti aziendali intelligenti.

Uno Smart Business Contract incorporerebbe regole complesse, processi, dati e webhook. Ma c'è ancora bisogno di un programma per incollare tutti i componenti insieme e orchestrare il loro lavoro. Ciò richiede un linguaggio di programmazione generale e completo di Turing. Potremmo supportarlo con la macchina virtuale CyberMiles che verrà spedita con il software blockchain su ogni nodo di rete.

2.3 Modelli di contratto Business Ready

Un aspetto chiave dello Smart Business Contract è che i contratti non sono solo costruiti su componenti software riutilizzabili, ma anche riutilizzabili. Poiché la maggior parte degli scenari di transazioni commerciali sono ben definiti (sia dal punto di vista legale che commerciale), è possibile creare modelli di contratti aziendali intelligenti che possono essere riutilizzati cambiando solo i termini chiave come parametri (ad esempio, nomi di parti del contratto, date, importi eccetera.). Questa libreria di modelli ridurrebbe il costo di creazione e distribuzione di applicazioni aziendali e aumenterebbe il valore della rete stessa.

2.4 App decentralizzate con Smart Business Contracts

Nel sistema di blockchain CyberMiles, esiste ancora un concetto di applicazioni decentralizzate (DApps). A CyberMiles DApp gestirà tutti i dati e la logica che non dovrebbero essere memorizzati sulla blockchain per motivi di privacy o di prestazioni. La logica di business relativa alla transazione commerciale potrebbe essere completamente trasferita allo Smart Business Contract.

3. TECNOLOGIA

Le soluzioni tecnologiche per lo stack middleware della blockchain di CyberMiles sono relativamente semplici, in quanto sono tutte tecnologie già ampiamente utilizzate nel mondo del middleware aziendale. Stiamo costruendo una soluzione ingegneristica per incorporare tali tecnologie nel framework blockchain e progettare incentivi economici adeguati affinché il sistema funzioni.

I quadri tecnologici specifici discussi in questo documento sono solo a scopo illustrativo. La comunità potrebbe organizzare una discussione e un evento di votazione in una data successiva per eleggere un comitato governativo sulla tecnologia, che poi determinerebbe collettivamente le esatte scelte tecnologiche per lo stack middleware CyberMiles.

3.1 Il motore delle regole

Il sistema CyberMiles incorporerà un motore di regole di inferenza che collega in avanti il suo software validatore della blockchain . Il motore delle regole risiede al di fuori della blockchain stessa ma viene utilizzato dal validatore(o miner) per eseguire Smart Business Contracts.
Il motore delle regole implementa l'algoritmo di rete per associare i modelli (fatti dalle azioni aziendali) alle regole e risolvere potenziali conflitti. L'algoritmo di rete è complesso e al di là dello scopo di questo documento.
Vogliamo sottolineare che, tuttavia, esistono motori di regole di concatenamento a termine basati su reti mature e di successo ampiamente utilizzati nelle imprese di oggi. Esempi di tali motori di regole includono Drools e Jess. A livello concettuale, le regole di concatenamento in avanti sono un insieme complesso di istruzioni IF e THEN. Il motore delle regole offre uno speciale "linguaggio di programmazione" che consente agli analisti aziendali, al contrario degli sviluppatori di software, di esprimere le regole aziendali. L'esempio seguente mostra un insieme di regole scritte in un linguaggio di pseudo regole. Mostra come determinare il prezzo di un prodotto in base al profilo dell'acquirente. In questo caso, se il punteggio FICO dell'acquirente è superiore a 740, gli verrà offerto uno sconto dell'80% sul prezzo.

```
Rule “Pricing”
dialect “mvel”
when
m : Message(status==Message.GET_PRICE)
then
when
m.fico_score > 740
then
```

```
m.price = m.listed_price * 0.8
End
```

Lo Smart Business Contract può ora eseguire le regole quando viene invocato da DApps. Si noti che i dati richiesti per il "profilo dell'acquirente" e il prezzo del prodotto vengono recuperati da un database distribuito sulla piattaforma CyberMiles, che esamineremo ulteriormente nella Sezione 3.3

```
engine = load_rules("pricing.rl");
m = new Message ();
m.status = Message.GET_PRICE;
m.fico_score = 741; // Get from profile DB
m.listed_price = 100; // Get from product DB 15
engine.send(m);
return m.price; // Returns 80 to Dapp caller
```

Mentre questo esempio è semplice, è illustrativo. È facile vedere come lo Smart Contract Business può gestire regole complesse e incapsulare gran parte della logica di business nel sistema.

3.2 Il Business Process Manager (BPM)

Nella maggior parte dei sistemi aziendali, le regole vengono applicate in modo reattivo solo quando vengono soddisfatte determinate condizioni. Ad esempio, la regola di determinazione del prezzo del prodotto viene applicata solo quando un potenziale acquirente chiede il prezzo (ad esempio, caricando la pagina web con i dettagli del prodotto). In questo senso, il motore delle regole viene invocato "su richiesta" e il sistema passa molto del suo tempo in uno stato di "attesa". Questo comportamento può essere modellato da una macchina a stati finiti (FSM).

Una classe di prodotti software aziendali ampiamente utilizzata che implementa l'FSM è nota come Business Process Manager (BPM). Il BPM fornisce anche il proprio linguaggio dichiarativo per l'analista aziendale per specificare il processo. Ogni stato può corrispondere a una regola aziendale per determinare come attivare lo stato successivo. Il linguaggio BPM è spesso basato su XML. L'esempio seguente mostra un sottoinsieme di stati che un BPM potrebbe gestire in un tipico scenario di commercio elettronico.

```
<process-definition name=”purchase process”>
<start-state name=”request a purchase”>
<transition to=”evaluate”/>
</start-state>
<state name=”evaluate”>
<!--...-->
<transition name=”approve” to=”approved”/>
<transition name=”disapprove” to=”done”/>
</state> 16 <fork name=”approved”>
<transition to=”decrement inventory” />
<transition to=”credit seller” />
<transition to=”deduct from buyer” />
</fork>
<state name=”decrement inventory”>
<!--...-->
<transition to=”done” />
</state>
<state name=”credit seller”>
<!--...-->
<transition to=”done” />
</state>
<state name=”deduct from buyer”>
<!--...-->
<transition to=”done” />
</state>
<end-state name=”done” />
</process-definition>
```

Lo script BPM può manipolare variabili, avviare o terminare attività parametrizzate o anche fare riferimenti al motore delle regole esterne.
La programmazione nello script Smart Business Contract può ora essere semplificata in una serie di dichiarazioni dichiarative per verificare lo stato di FSM.

```
// pid is the ID of a process
// associated with a shopping session
// It is stored in the distributed DB
if (pid) {
process = load_process (pid);
} else {
process = start_process(“purchase.bpm”);
pid = process.id;
// Save pid to the DB
}
17
while (process.next()) {
if (process.state == “credit seller”) {
// Do the transaction …
}
if (process.state==”deduct from buyer”) {
// Do the transaction …
}
… …
```

}

Le soluzioni BPM di middleware enterprise ampiamente utilizzate includono jBPM, Enhydra Shark e OpenSymphony OSWorkflow.

3.3 Il database distribuito

Sia il motore delle regole che il BPM devono memorizzare i dati interni in un database per funzionare in modo efficiente. Poiché l'applicazione aziendale cresce in complessità, l'applicazione stessa deve anche gestire i dati al di fuori dei record di transazione nella blockchain. Ciò richiede un database incorporato in tutti i nodi blockchain. A causa della naturale distribuzione delle applicazioni blockchain, questo nodo deve anche essere replicato e sincronizzato su tutti i nodi blockchain.
Fortunatamente, le tecnologie di database distribuite hanno visto grandi progressi negli ultimi anni. È ora possibile creare database distribuiti su scala Internet utilizzando software open source disponibili in commercio. Tuttavia, il compromesso è che quei database sono in genere NoSQL e non possono garantire la coerenza del sistema in un dato momento. Al contrario, mirano a una "coerenza finale" in quanto il sistema risolve gradualmente potenziali conflitti. Adottano una strategia di risoluzione dei conflitti molto diversa ma utile rispetto alla blockchain stessa.
Abbiamo deciso in via preliminare di utilizzare il popolare Apache Cassandra come database distribuito predefinito per CyberMiles.

3.4 Il file system distribuito

Lo Smart Business Contract ha spesso bisogno di gestire file o blocchi di dati oltre a blockchain e database. Questi file devono essere replicati e accessibili attraverso i nodi sulla blockchain. Pertanto, è necessario un file decentralizzato e un sistema di archiviazione dei dati.

Il sistema CyberMiles utilizzerà tecnologie di file system distribuite a misura di blockchain come Ethereum Swarm e IPFS come struttura di archiviazione di file standard.

3.5 I Webhook distribuiti

Come evidenziato sopra, il sistema aziendale reagisce agli eventi esterni. Il BPM attende input da parte dei contraenti (noto come "oracolo" per lo stato mondiale esterno). Quindi invoca le regole per determinare cosa fare dopo. Dopo aver raggiunto lo stato successivo, attende di nuovo l'input. Poiché l'infrastruttura di e-commerce si trova su Internet, il sistema CyberMiles deve disporre di un'interfaccia per ricevere eventi da Internet.

Per fare ciò, ciascun nodo blockchain di CyberMiles incorpora anche un server Web che può ricevere messaggi esterni e attivare eventi BPM. Ciascuna applicazione Smart Business Contract può pubblicare uno o più URL Webhooks per ricevere eventi esterni. I nodi attivi sulla blockchain si registrano sul sistema DNS e possono ricevere tutte le richieste HTTP in entrata.

4. BLOCKCHAIN

Uno Smart Business Contract unisce tutti i componenti del middleware aziendale e li collega al registro delle transazioni gestito dalla blockchain. Seguendo la guida di Ethereum, CyberMiles sta costruendo una macchina virtuale completa di Turing collegata alla blockchain. La macchina virtuale può essere programmata tramite un linguaggio di scripting simile a JavaScript (simile al linguaggio di programmazione Solidity di Ethereum). Può completare attività quali la connessione di eventi Webhook ai processi BPM, il caricamento di regole aziendali e l'accesso ai database condivisi (vedere la Figura 1).Per uno Smart Business Contract, lo sviluppatore dovrebbe riunire insieme il codice dell'applicazione, i file di configurazione BPM, la configurazione webhook e il file delle regole aziendali in un singolo archivio e quindi inviare il file di archivio alla blockchain per l'elaborazione e la distribuzione. Una volta implementato lo Smart Business Contract, i sistemi esterni possono accedervi tramite indirizzi blockchain. Ad esempio, DApps può creare un'interfaccia utente per

l'applicazione e utilizza Smart Business Contract per elaborare tutta la logica aziendale e registrare le transazioni token risultanti nella blockchain.

4.1 Blockchain e consenso

Per il livello blockchain del sistema CyberMiles, miriamo NON a reinventare la ruota, ma a costruire su una struttura di blockchain esistente. I nostri criteri principali per la tecnologia di base includono quanto segue.

- Deve essere un progetto open source guidato dalla comunità e attivamente sviluppato. Ciò consentirebbe a CyberMiles di apportare modifiche al software dell'infrastruttura, influenzare le direzioni future del software e contribuire alla comunità.

- L'architettura del software deve supportare una netta separazione tra la logica del blockchain core (cioè la logica del consenso) e la logica dell'applicazione per convalidare le transazioni. Il motore del consenso si prende cura del processo per proporre e impegnare nuovi blocchi sulla catena; Le applicazioni personalizzate convalidano le transazioni, inclusa l'esecuzione degli Smart Business Contracts, e determinano quali transazioni devono essere registrate nella blockchain. La macchina virtuale CyberMiles e l'intero stack software per Smart Business Contracts sarebbero scritti come applicazioni personalizzate sulla blockchain.
- Il motore di consenso blockchain deve avere prestazioni comprovate per adattarsi a applicazioni di livello consumer con milioni di utenti. Idealmente, dovrebbe essere una delle migliori soluzioni riconosciute per la scalabilità di Ethereum. In altre parole, deve essere leader di mercato in termini di maturità ingegneristica.

Il team di CyberMiles ha condotto ricerche approfondite confrontando le soluzioni di infrastruttura blockchain disponibili. Abbiamo provvisoriamente concluso che costruiremo la prima iterazione della blockchain CyberMiles sulla piattaforma Tendermint / Cosmos. La Figura 2 mostra

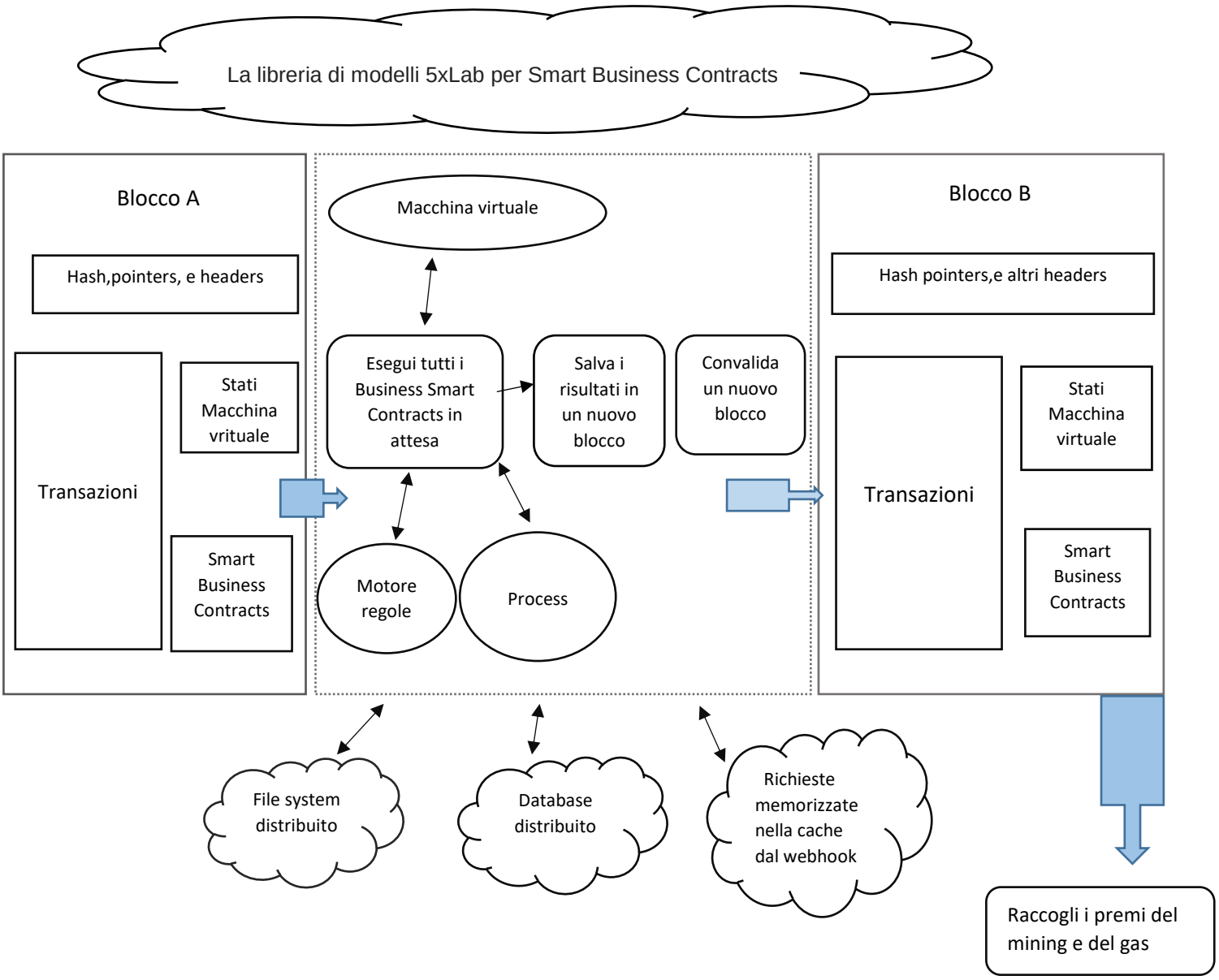
l'architettura software proposta su ciascuno dei nodi di validazione sulla blockchain di CyberMiles. Infatti, CyberMiles sta già apportando contributi tecnici alla piattaforma Tendermint / Cosmos.

• Il progetto Tendermint crea un motore di consenso bizantino con tolleranza ai guasti "Bizantine Fault Tolerance" (BFT). È uno sforzo open source molto attivo e ben finanziato (dopo una ICO di successo). La blockchain stessa può resistere fino a 1/3 del guasto del nodo (arrestato o sovvertito). In una configurazione DPoS (Delegated Proof of Stake), i singoli validatori sono fortemente incentivati a sovvertire la rete, rendendo i ritorni bizantini estremamente rari.

• Tendermint ha un'architettura moderna e modulare. Il motore del consenso può essere collegato in modo indipendente ad altri tipi di blockchain. Ad esempio, il progetto Ethermint utilizza il motore di consenso di Tendermint per scalare Ethereum. L'ABCI (Applicaion BlockChain Interface) è un'interfaccia logica di applicazione semplice e pulita che consente a CyberMiles di sviluppare la sua macchina virtuale e lo stack di applicazioni. All'arrivo di una nuova transazione, la blockchain passerebbe all'applicazione CyberMiles tramite ABCI; Una volta eseguiti gli Smart Business Contracts rilevanti e la transazione viene convalidata dall'applicazione CyberMiles, questa verrà restituita al motore di consenso blockchain per la conservazione dei record.

• Tendermint è un'implementazione blockchain ad alte prestazioni basata sul meccanismo di consenso DPoS (Delegated Proof of Stake). È ufficialmente approvato da Ethereum come soluzione di scalabilità di Ethereum. Durante i test, può supportare in modo affidabile 10.000 transazioni al secondo, rendendolo una delle soluzioni ingegneristiche più avanzate.

A causa del sottostante meccanismo Tendermint DPoS, la blockchain CyberMiles avrebbe un tempo di generazione del blocco inferiore a 10 secondi e le transazioni in un blocco vengono confermate all'istante una volta che il blocco è stato eseguito.



La Figura 2. illustra il lavoro svolto dai validatori di blockchain CyberMiles.

4.2 Il token crittografico

La blockchain CyberMiles creerà e registrerà un token crittografico nativo chiamato CyberMiles Token (CMT). Ci sono due usi del CMT: compensare i membri della comunità per i servizi che

forniscono e facilitare le transazioni finanziarie sulla rete. Questi due casi d'uso sono anche correlati tra loro in quanto la "commissione" raccolta da ogni transazione è utilizzata per pagare i validatori che forniscono servizi per facilitare la transazione. Consideriamo ora i due casi d'uso in dettaglio. In primo luogo, i partecipanti alla rete possono guadagnare CMT fornendo servizi.

• Potrebbero diventare validatori per servire la rete. Nello specifico, i partecipanti eseguono contratti aziendali intelligenti per DApp (come l'app 5miles) per guadagnare CMT (gas pagato dalle DAapps, vedi sotto). Oppure, potrebbero convalidare e registrare nuove transazioni sulla blockchain e guadagnare CMT dal protocollo di consenso DPoS.

• Potrebbero fornire servizi ai loro colleghi sulla rete. I consumatori e le imprese sulla rete potrebbero utilizzare CMT per pagarsi a vicenda per servizi, come i servizi di arbitrato per la risoluzione delle controversie e persino i servizi di sviluppo per i contratti aziendali intelligenti

Nota: la CMT verrebbe convertita in gas a un tasso di cambio dinamico, in modo che il valore convertito di un'unità di gas rimanga stabile. Il gas viene quindi utilizzato per pagare i nodi CyberMiles che eseguono gli Smart Business Contracts. Il prezzo del gas del Contratto Smart Business verrà stimato dal sistema nel momento in cui il Contratto Smart Business viene presentato alla blockchain. In secondo luogo, la CMT potrebbe essere utilizzata come valuta di regolamento interna sulle applicazioni di rete CyberMiles. Ad esempio, una richiesta di prestito per piccole imprese (vedere la sezione 5) potrebbe utilizzare CMT per regolare prestiti e rimborsi senza una stanza di compensazione centralizzata per garantire la privacy, la trasparenza e la sicurezza dei fondi; Un'applicazione di gestione della catena di fornitura potrebbe regolare le transazioni intermedie in CMT e consentire solo la conversione in valute legali per i saldi alla fine di un giorno. Ciò riduce la finzione e i costi di transazione. In entrambi i casi, la rete estrae una piccola commissione da ciascuna

transazione di regolamento per pagare i validatori che eseguono gli Smart Business Contracts relativi alla transazione.

Entrambi i casi d'uso del CMT sono ben accettati nella comunità tecnologica blockchain. Il CMT è necessario perché stiamo costruendo una nuova infrastruttura blockchain CyberMiles, e quindi non possiamo semplicemente usare ETH o BTC per le funzioni native della nuova blockchain. La CMT può essere confrontata con alcuni token popolari che esistono oggi.

Confronto con XRP

Come la rete di Ripple, la rete CyberMiles utilizza il suo token crittografico nativo per facilitare il regolamento decentrato delle transazioni.

Tuttavia, Ripple "brucia" una piccola quantità di XRP per ogni transazione mentre CyberMiles raccoglie la commissione di transazione per pagare i validatori che eseguono gli Smart Business Contracts associati alla transazione. Inoltre, la rete di Ripple è una blockchain basata su permessi e tutti i nodi sono grandi istituzioni finanziarie. La rete CyberMiles sarebbe una blockchain pubblica che serve le piccole imprese.

Confronto con ETH

Come la rete Ethereum, la rete CyberMiles premierà i validatori sia per la creazione di nuovi blocchi che per l'esecuzione degli Smart Contracts nel blocco (tramite le tariffe del gas).

Tuttavia, l'attuale generazione di Ethereum è molto lenta e quindi proibitivamente costosa per eseguire contratti intelligenti complessi. CyberMiles è progettato per essere altamente performante e scalabile per l'esecuzione di complessi contratti aziendali intelligenti. Inoltre, Ethereum si propone di essere una rete informatica generica, mentre i Smart Business Contratti CyberMiles sono specificamente ottimizzati per le transazioni di e-commerce.

4.3 Avvia l'effetto rete

Per far decollare la rete CyberMiles, è essenziale raggiungere l'effetto di rete e fornire un valore sufficiente alle imprese e ai minatori per unirsi alla rete. Uno degli scopi di un ICO è fornire risorse per far ripartire la rete. Miriamo a realizzare quanto segue attraverso l'ICO di CyberMiles.

Innanzitutto, il team di sviluppo sfrutterà la vasta esperienza di 5Miles nella gestione di uno dei più grandi siti Web di e-commerce negli Stati Uniti per creare modelli di contratti aziendali intelligenti. Ci sono migliaia di modelli di contratto in 5Miles divisi in 20 categorie principali. Sono testati per applicazioni del mondo reale e sono prontamente disponibili per il riutilizzo. Inoltre, il sistema opera a "Store", che è di per sé un DApp su blockchain, per vendere modelli di Smart Business Contract sviluppati da utenti di terze parti. I modelli possono essere prezzati in CMT o in unità gas.

In secondo luogo, 5miles creerà una nuova applicazione per supportare i prestiti alle piccole imprese tra i suoi 10 milioni di utenti statunitensi e le piccole imprese. L'applicazione sosterrà l'identità personale decentralizzata e la gestione del credito, nonché il regolamento decentrato di prestito / rimborso (senza una stanza centrale di compensazione). Questo sforzo potrebbe potenzialmente trasferire 10 milioni di identità utente americane e storie creditizie alla blockchain di CyberMiles. Questa applicazione potrebbe fornire un piano per altri sviluppatori per sfruttare l'identificazione degli utenti e la cronologia dei crediti su CyberMiles e creare le proprie applicazioni per i consumatori. Usando la CMT come valuta di regolamento, la rete CyberMiles può prelevare una piccola commissione per pagare i validatori per l'esecuzione di contratti aziendali intelligenti relativi ai termini dei prestiti. Con l'aumento delle applicazioni su CyberMiles, il consumo di gas CMT aumenterà.

Infine, 5miles trasferirà l'applicazione di commercio elettronico Flagship C2C (Consumer to Consumer) di punta alla blockchain CyberMiles. Sarà un DApp gestito da 5miles e supportato da Smart Business Contracts su CyberMiles. Ciò potrebbe potenzialmente trasferire transazioni per $ 3 miliardi alla piattaforma CyberMiles. Di conseguenza, 5miles stesso acquistera' e consumera' una

quantità significativa di CMT per pagare il costo del gas per la gestione degli Smart Business Contracts.

5. APPLICAZIONI

La piattaforma blockchain CyberMiles supporta principalmente le operazioni di middleware per le applicazioni transazionali di business. In quanto tale, sarebbe per lo più al di sotto dell'interfaccia utente dell'applicazione utente. Tuttavia, a causa delle caratteristiche uniche della blockchain decentralizzata, i suoi Smart Business Contracts potrebbero consentire potenziali nuove funzionalità e applicazioni che non erano possibili nel mondo delle operazioni di e-commerce centralizzato.

5.1 Una piattaforma di gestione di identificazione decentralizzata

Come dimostrato dalla Equifax hack (identificazione personale e storia del credito di oltre 100 milioni di americani sono stati rubati nel 2017), la gestione centralizzata dell'identità personale crea un alto rischio per i consumatori e un'alta responsabilità per le aziende che detengono tali dati. Per risolvere questo problema, è necessario riconsiderare l'intero paradigma della gestione dell'identità. Una soluzione ovvia è lasciare che l'utente abbia il pieno controllo delle sue informazioni personali. L'utente dovrebbe essere in grado di decidere, caso per caso, chi ha accesso ai suoi dati. Il tempo di accesso, la durata e l'uso accettato dei dati dovrebbero essere tutti approvati dall'utente. In questo caso, non ci sarà alcun repository centrale di informazioni personali da attaccare. Tuttavia, senza gli Smart Business Contracts basati su blockchain, tali sistemi sono anche molto difficili da implementare.

Le reti blockchain gestiscono le identità tramite chiavi crittografiche. I "portafogli" dell'utente su bitcoin o blockchain Ethereum sono decentralizzati e interamente controllati dall'utente tramite la propria chiave privata. Utilizzando gli Smart Business Contracts, possiamo estendere il concetto di "portafogli" per includere un deposito sicuro non solo di token crittografici, ma anche di informazioni personali arbitrarie. Come i portafogli crittografici, potrebbero esserci molti "portafogli personali"

sulla rete. Su richiesta dell'utente (transazione firmata dalla chiave privata dell'utente), il wallet può autorizzare applicazioni di terze parti ad accedere temporaneamente ai dati tramite il protocollo OAUTH. Un utente può utilizzare diversi portafogli per scopi diversi, proprio come oggi vengono utilizzati i portafogli crittografici token.

Il flusso di lavoro sotto e la Figura 3 illustrano come un "portafoglio online" per le informazioni personali potrebbe funzionare. Questo particolare "portafoglio" memorizza le informazioni bancarie personali dell'utente. Quindi l'utente può autorizzare applicazioni finanziarie sulla rete CyberMiles per utilizzarlo. Un esempio è l'applicazione peer-to-peer per il prestito alle piccole imprese illustrata nella Sezione 5.2.

1. L'utente seleziona un'app "wallet" di cui si fida.

2. L'utente registra le informazioni personali e le informazioni bancarie con il portafoglio.

3. Il portafoglio esegue convalide AML / KYC per il controllo della lavanderia anti-money imposto dal governo.

4. Il wallet genera una coppia di chiavi pubblica / privata e quindi trasmette la chiave pubblica alla blockchain per la registrazione.

5. Il portafoglio autorizza e verifica il collegamento bancario.

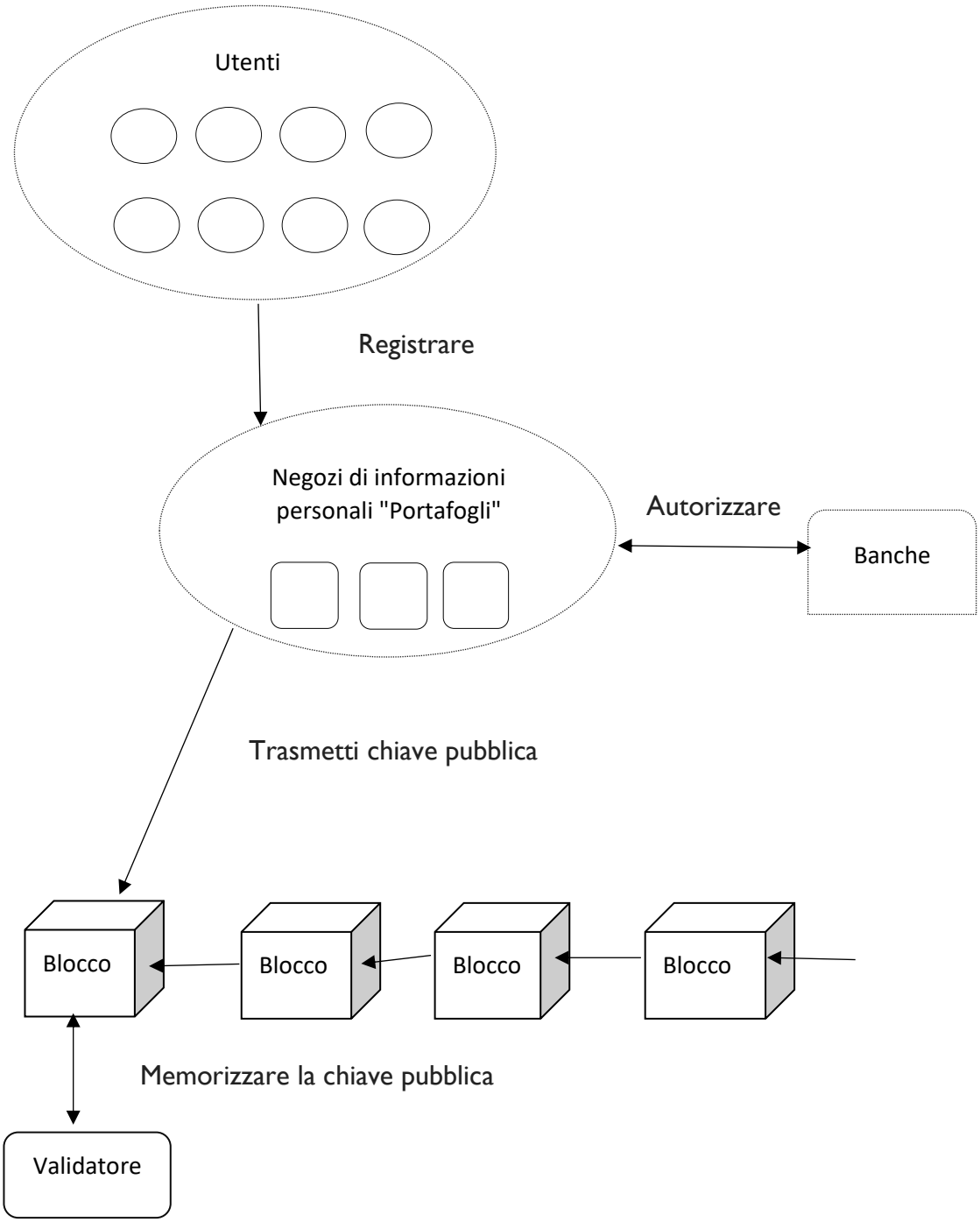


FIGURA 3. UNA PIATTAFORMA DECENTRALIZZATA DELLE GESTIONE DELL'IDENTITÀ SU CYBERMILES

5.2 Un mercato dei prestiti per le piccole imprese peer-to-peer

Una potenziale applicazione creata sulla blockchain di CyberMiles sarebbe un mercato di prestiti alle piccole imprese peer-to-peer. Come descritto nella sezione 5.1, costruiremo una piattaforma di

gestione delle identità decentralizzata su CyberMiles. La blockchain può quindi registrare la cronologia dei crediti per ciascun utente identificato dalla sua chiave pubblica.

Con la storia dell'identità e del credito, possiamo costruire un motore di matching del prestito (il "cambio" del prestito) sulla blockchain. E una volta che i termini del prestito sono stati abbinati, gli Smart Business Contracts regolerebbero automaticamente il prestito direttamente dal conto bancario di ciascuna delle parti utilizzando CMT (autorizzato tramite i loro "portafogli di informazioni personali") senza una stanza centrale di compensazione. Il flusso di lavoro sottostante e la Figura 4 descrivono come abbinare e regolare un prestito.

1. L'utente accede allo scambio tramite OAUTH dal suo portafoglio. Lo scambio memorizza nella cache ma non memorizza le informazioni personali.

2. L'utente invia i suoi termini di prestito desiderati (prestiti o prestiti, termini, tassi di interesse).

3. Lo scambio suggerisce le partite.

4. Lo scambio fornisce punteggi e storie di credito dettagliati per i candidati abbinati.

5. Se l'utente seleziona un candidato. Entrambe le parti dovranno essere d'accordo.

6. Il contratto di prestito è registrato dallo scambio e sulla blockchain.

7. Lo scambio richiede ai portafogli di regolare entrambe le parti tramite i loro conti banca

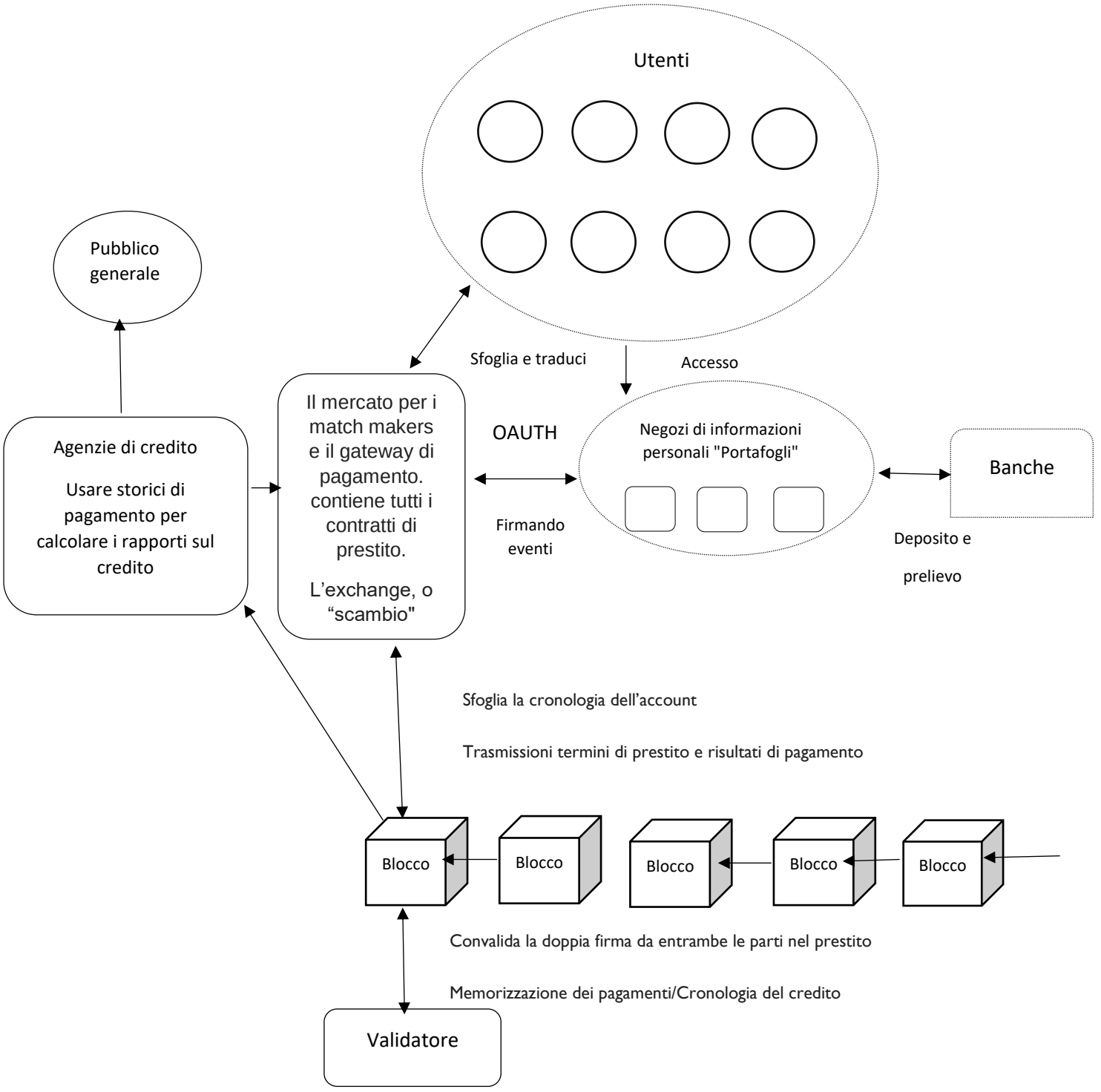


FIGURA 4. ABBINARE E REGOLARE UN PRESTITO DECENTRALIZZATO.

Per tutta la durata del prestito, quando un pagamento è dovuto, il Contratto Smart Business eseguirà automaticamente quanto segue.

1. Lo scambio richiede ai portafogli di entrambe le parti di regolare i pagamenti tramite i loro conti bancari.

2. Il risultato della transazione viene trasmesso alla blockchain e diventa parte della cronologia dei crediti.

5.3 Flusso di cassa della catena di fornitura

Il token virtuale nel sistema blockchain CyberMiles (CMT) viene utilizzato principalmente per compensare l'accesso alla rete (ad esempio, le aziende pagano per eseguire la propria Smart Business Contract e convalida della rete blockchain). Tuttavia, potrebbe anche essere utilizzato come mezzo in rete per regolare i conti delle parti, compresi i consumatori finali e i venditori, sulla catena di approvvigionamento.

Poiché CMT è un token digitale, il suo insediamento sarebbe istantaneo, gratuito e sicuro. Il CMT consente una gestione della catena di approvvigionamento estremamente efficiente, poiché il "flusso di transazioni" potrebbe avvenire contemporaneamente al movimento dei prodotti. Le parti avrebbero solo bisogno di convertire periodicamente il loro saldo CMT in altre attività attraverso gli scambi sulla rete.

5.4 Prodotti certificati

Una delle caratteristiche chiave della blockchain è la sua capacità di conservare record digitali immutabili e sicuri. Questa funzione aiuta ad affrontare uno dei problemi più difficili nell'e-commerce globale: i prodotti contraffatti.

È possibile impostare Smart Business Contracts per produttori / produttori di prodotti per creare certificati di autenticità per ciascuno degli articoli del prodotto che producono (ad es. Tramite una connessione API tra il sistema di produzione dello stabilimento e lo smart contract business CyberMiles). Questo certificato potrebbe quindi essere tracciato in modo trasparente mentre il prodotto passa attraverso la catena di approvvigionamento dai venditori agli acquirenti.

5.5 Risoluzione delle controversie basata sulla comunità

Una società di e-commerce centralizzata ha bisogno di assumere i servizi clienti per risolvere le controversie tra acquirenti e venditori. Una società di e-commerce che costruisce un DApp in cima alla blockchain di CyberMiles potrebbe ovviamente fare lo stesso. Tuttavia, in quanto piattaforma decentralizzata, CyberMiles offrirebbe un'altra soluzione convincente.

Gli utenti della comunità di CyberMiles potrebbero offrirsi come volontari per diventare arbitri in cambio di CMT. Poiché le fasi chiave della transazione sono registrate sulla blockchain (compresi i certificati di autenticità dei prodotti e le ricevute di consegna), un Contratto Smart Business potrebbe sviluppare un meccanismo con cui l'arbitro può individuare tali registrazioni con il consenso sia del venditore che dell'acquirente. Lo Smart Business Contract potrebbe mantenere un impegno di garanzia in CMT da parte del venditore e dell'acquirente in attesa della risoluzione del conflitto. Una volta che l'arbitro risolve il conflitto e entrambe le parti sono soddisfatte, l'impegno sarà rilasciato al partito "vincente" e l'arbitro riceverà un'assegnazione percentuale.

GLOSSARIO

CyberMiles blockchain: un nuovo protocollo blockchain decentralizzato ottimizzato per le transazioni commerciali.

Smart Business Contract: un'applicazione aziendale che può essere eseguita sulla blockchain di CyberMiles.

CyberMiles Token (CMT): Cryptocurrency / token utilizzato per assegnare persone che ospitano i nodi blockchain di CyberMiles per mantenere la blockchain ed eseguire contratti smart business. Le aziende e le parti che inoltrano smart contract di business da eseguire sulla rete devono pagare i CMT a seconda della complessità del contratto.

Convalida CyberMiles(validator o miner): una persona o entità che contribuisce alla potenza di calcolo per mantenere l'infrastruttura blockchain CyberMiles, incluso l'esecuzione di contratti aziendali intelligenti. Questa persona può essere ovunque nel mondo, e potrebbe non essere affiliato con 5 miglia. Lui / lei è incentivato dai premi (CMT che lui / lei può ricevere come sottoprodotto del mantenimento della rete).

Applicazione CyberMiles: qualsiasi azienda può creare e distribuire applicazioni sulla blockchain di CyberMiles. L'azienda presenterà una serie di Smart Business Contracts da eseguire sulla rete. L'azienda deve acquistare CMT per pagare la rete per l'accesso e potrebbe utilizzare le CMT per regolare o agevolare le transazioni finanziarie interne.

Utente finale: gli acquirenti e i venditori sull'applicazione 5miles non devono assolutamente conoscere CyberMiles. Gli Smart Business Contracts possono scambiare il proprio USD con / da CMT immediatamente prima e dopo la transazione.

5miles: si tratta di un'applicazione per il mercato e-commerce C2C (Consumer to Consumer) sviluppata da 5Miles LLC. 5Miles ha oltre 10 milioni di clienti statunitensi con un valore stimato di transazioni a rate annuali di $ 3 miliardi.

RINGRAZIAMENTI

Il 5xlab desidera ringraziare il Dr. Michael Yuan e il Dr. Lucas Lu per il loro contributo a questo documento.

RIFERIMENTI

[1] Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf 2008. 33

[2] The Ethereum Team. A Next-Generation Smart Contract and Decentralized Application Platform. https://github.com/ethereum/wiki/wiki/White-Paper 2014

[3] Kwon, J. Tendermint: Consensus without Mining. https://tendermint.com/static/docs/tendermint.pdf 2014.

[4] Popov, S. IOTA: The tangle. https://iota.org/IOTA_Whitepaper.pdf 2016.

[5] Zamfir, V. Introducing Casper "the Friendly Ghost". https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/ 2015.

[6] Kwon, J and Buchman, E. Cosmos: A Network of Distributed Ledgers. https://cosmos.network/whitepaper 2016.

[7] Wood, G. Polkadot: Vision for a heterogeneous multi-chain framework. https://github.com/polkadot-io/polkadot-white-paper 2016.

[8] Poon, J and Dryja, T. The Bitcoin Lightning Network:
Scalable Off-Chain Instant Payments. https://lightning.network/lightning-network-paper.pdf 2016.

[9] Poon, J and Buterin, V. Plasma: Scalable Autonomous Smart Contracts. http://plasma.io/plasma.pdf 2017.

[10] Teutsch, J and Reitwiebner, C. A scalable verification solution for blockchains. http://bit.ly/2vIConl 2017.

[11] Forgy, C. Rete: A Fast Algorithm for the Many Pattern / Many Object Pattern Match Problem. Artificial Intelligence. 19: 17–37. 1982.

[12] Oracle. The Java Enterprise Edition Platform. https://www.oracle.com/java/technologies/java-ee.html

[13] Redhat. The Drools Business Rules Management System. http://drools.org/ 34

[14] Sandia National Laboratories. Jess, the Rule Engine for the Java Platform. http://www.jessrules.com/

[15] Redhat. jBPM, a flexible Business Process Management Suite. http://www.jbpm.org/

[16] Lazo, D. OSWorkflow. http://shop.oreilly.com/product/9781847191526.do 2007

[17] DataStax. The Apache Cassandra database. http://cassandra.apache.org/

[18] The Ethereum Team. Swarm, serverless hosting incentivised peer-to-peer storage and content distribution. http://swarm-gateways.net/bzz:/theswarm.eth

[19] Benet, J. IPFS - Content Addressed, Versioned, P2P File System.

[20] Protocol Labs. Filecoin: A Decentralized Storage Network. http://filecoin.io/filecoin.pdf 2017.

[21] The Civic Team. Civic Whitepaper. https://tokensale.civic.com/CivicTokenSaleWhitePaper.pdf 2017

[22] Thomas, S. & Schwartz, E. A Protocol for Interledger Payments. https://interledger.org/interledger.pdf 2015