



Scrypta

Infrastruttura di archiviazione e certificazione

-LIGHT PAPER-

Indice

Prefazione	2
La Blockchain Oggi - <i>Analisi degli aspetti critici</i>	3
La Blockchain di Scrypta	5
Il Linguaggio di Scrypta - <i>Un accenno alle tecnologie</i>	6
Le Tre Macroaree di Scrypta	7
Aspetto Pratico - <i>Esempio di funzionamento</i>	8
Ambiti Applicativi - <i>Alcuni esempi di utilizzo</i>	9
Appendice I - I Parametri di Base di Scrypta	13
Appendice II - Piano di Distribuzione delle Ricompense	14
Appendice III - Roadmap	15

PREFAZIONE

Scrypta è un'infrastruttura Peer-to-Peer ideata per nuovi modelli di business e di gestione delle P.A. Il sistema si basa sull'emissione di valuta digitale detta '**LYRA**'. Scrypta include funzionalità decentralizzate avanzate per una maggiore scalabilità e flessibilità e per la creazione di architetture complete a servizio di progetti illimitati e nuovi casi d'uso. L'algoritmo che regola Scrypta garantisce uno schema di transazioni ad alta velocità per trasferimenti di asset digitali e pagamenti istantanei. Lo schema di emissione monetaria, e quindi di ricompense, si basa sull'algoritmo **Quark** che incorpora un layer di consenso ibrido **PoS/Masternode** energeticamente efficiente e particolarmente sicuro.

Scrypta è un progetto in continua evoluzione. La sua natura decentralizzata lo rende particolarmente adatto alle collaborazioni e ai contributi di sviluppatori che vorranno creare soluzioni pratiche basate sulla sua architettura. L'ecosistema progettato intorno a Scrypta, inoltre, offre mezzi eccezionali di archiviazione, certificazione e verifica che rappresentano ottimi strumenti per tutte quelle aziende desiderose di affacciarsi all'innovazione tecnologica offerta dalla blockchain.

Scrypta nasce dall'idea di un gruppo coeso di innovatori. Al rilascio del White Paper, previsto a fine gennaio 2019, forniremo maggiori dettagli in merito alla composizione del Core Team.

Tutto quello che leggerete in questo documento è realmente funzionante, non si tratta del progetto visionario di una startup: il codice è già sviluppato, testato ed operativo.

Potete richiedere una dimostrazione inviando una mail a: info@scryptachain.org

LA BLOCKCHAIN OGGI

Analisi degli aspetti critici

- Il 2017/2018 è stato un biennio cruciale per lo sviluppo dell'intero ecosistema blockchain. Le aziende e le startup si sono però troppo concentrate sugli aspetti lucrativi e finanziari mettendo in secondo piano il linguaggio e le potenzialità della blockchain stessa.
- L'avvento di Ethereum come sistema di creazione e mantenimento di codice (definito anche Smart Contract) non ha ancora raggiunto l'adozione capillare che ci si aspettava. Il suo enorme potenziale risiede proprio negli Smart Contract e nella loro implementazione in casi d'uso reale. Attualmente invece, questi strumenti vengono utilizzati principalmente per la mera emissione di token a scopi finanziari.
- Tra le circa 2000 digital coin presenti sul mercato, molte non hanno reali casi d'uso ed hanno visto deprezzare il proprio valore fino al 90%, creando così un malumore diffuso tra gli investitori, soprattutto i medio-piccoli.
- L'attenzione per le dApp (Applicazioni Decentralizzate che sfruttano la tecnologia blockchain) e per la sicurezza intrinseca che offrono - non possedendo fisicamente i dati degli utenti - è salita enormemente: non solo gli addetti ai lavori, ma anche molte persone comuni sono ormai consapevoli del fatto che i classici servizi "data-centrici" rappresentano un passato destinato a sparire in favore di un'architettura che permette un alto livello di privacy e di controllo dell'utente sui propri dati.
- Il linguaggio della blockchain, così come quello di altre tecnologie, è complesso. Il ruolo vincente delle aziende e degli sviluppatori è

dunque quello di rendere la tecnologia accessibile, creando servizi semplici che risolvono problemi reali.

- La focalizzazione sulla risoluzione dei problemi reali è la chiave per il successo dell'intero ecosistema, fin quando non si potrà utilizzare questa tecnologia comodamente nella vita di tutti i giorni, allora essa continuerà ad essere un fenomeno di nicchia. Il nostro compito è quello di trasmettere e costruire le infrastrutture tecniche a supporto di una diffusione capillare della tecnologia blockchain.

LA BLOCKCHAIN DI SCRYPTA

LYRA

Lo scambio e l'inserimento dei dati nell'infrastruttura di Scrypta avviene grazie alle transazioni operate in LYRA. LYRA è un "digital asset" e non un "token" poichè dispone di una blockchain proprietaria detta Scrypta. Il costo operativo per l'inserimento dei dati nella blockchain di Scrypta è di millesimi di LYRA ad operazione. Questo permette la costruzione di infrastrutture complesse su una base solida ma al contempo accessibile e dai costi contenuti.

PoS (Proof-of-Stake)

L'algoritmo di consenso Proof-of-Stake utilizzato da Scrypta agisce per convalidare le transazioni e ottenere il consenso distribuito. Con il Proof of Stake, il creatore di un nuovo blocco viene scelto in modo deterministico a seconda della sua 'ricchezza', definita come 'stake'. L'algoritmo di consenso di Scrypta seleziona un validatore ogni 60 secondi e assegna a quel validatore il diritto di creare un singolo blocco. La catena di blocchi si basa quindi su nodi incentivati a mantenere una partecipazione economica nella rete. In altre parole, significa che i

“portafogli digitali” aperti alla rete, coniano nuove monete e assicurano un reddito passivo.

Gli sviluppatori e la comunità di Scrypta sfruttano il Proof of Stake per una forma di consenso distribuita più "verde" e quindi meno costosa. Grazie al sistema PoS, i validatori non devono usare la loro potenza di calcolo perché gli unici fattori che influenzano le loro possibilità di essere ricompensati sono il numero delle loro monete “bloccate” e la sana competizione fra stakeholder.

Masternode

Un masternode è un server, online 24 ore su 24, 7 giorni su 7, che opera come super validatore e per questo viene ricompensato in LYRA. I masternodes eseguono funzioni di nodo standard come l'hosting di una copia della blockchain e la convalida delle transazioni sulla rete, e inoltre agiscono come azionisti, votando proposte per migliorare l'ecosistema di Scrypta. I Masternode permettono anche altre importanti funzioni come “SwiftX” per l'invio istantaneo e “Obfuscation” per aumentare la privacy degli utenti.

Operare come validatore masternode richiede la proprietà di 15000 LYRA. I Masternodes devono inoltre avere un indirizzo IP statico e soddisfare i requisiti minimi per CPU, RAM, spazio su disco e larghezza di banda della rete.

IL LINGUAGGIO DI SCRIPTA

Un accenno alle tecnologie

Ogni applicazione, sia essa centralizzata o decentralizzata, necessita di due entità fondamentali: dati (file) e archiviazione (database). Attraverso Scripta è possibile inserire dati nella blockchain e creare sistemi complessi e decentralizzati di archiviazione.

Scripta ha sviluppato delle tecniche innovative di interfacciamento con la blockchain che permettono agli sviluppatori di ideare specifiche applicazioni decentralizzate utilizzando i linguaggi standard di programmazione per il web. Questa sfera viene principalmente rappresentata dalle speciali **API RESTful**, realizzate per l'inserimento e la lettura di informazioni nella Blockchain di Scripta.

In particolare la struttura poggia su quelli che abbiamo definito **Interconnected dApp Node (IdA Node)** che recepiscono i più comuni linguaggi di sviluppo come PHP, NodeJS e MongoDB e servono sostanzialmente a decifrare tutte le operazioni sottintese e complesse che vengono svolte dall'utilizzatore finale di un'applicazione.

Gli ideatori di Scripta inoltre, attraverso l'unione degli IdA Node e dei Masternode, hanno disegnato una infrastruttura di base su cui poggiare la tecnologia **IPFS (Inter Planetary File System)**: un'innovativa tecnica per creare archivi decentralizzati e distribuiti in grado di contenere permanentemente grosse quantità di dati, file e hypermedia.

Riassumendo, Le tecnologie e i linguaggi sfruttati da Scripta sono:

- **La Blockchain di tipo MN/PoS** (Masternode/Proof of Stake), diffusa e ben testata contro attacchi di varia natura.

- **I Nodi di interfacciamento 'IdA Nodes'**, che recepiscono i più comuni linguaggi di sviluppo come PHP, NodeJS e MongoDB e servono sostanzialmente a decifrare tutte le operazioni sottintese e complesse che vengono svolte dall'utilizzatore finale di una applicazione decentralizzata.
- Comune **linguaggio Web**, che ha come fine la realizzazione dell'interfaccia per l'utente e che viene principalmente rappresentato da Javascript e dalle speciali API RESTful, realizzate per l'inserimento e la lettura di informazioni nella Blockchain di Scrypta.

LE TRE MACROAREE DI SCRYPTA

Infrastructure & Protocol Provider – Scrypta fornisce un'infrastruttura Blockchain sulla quale costruire piattaforme sicure.

Application e Solution Provider – il team di Scrypta è specializzato nella realizzazione di applicazioni che prevedono l'utilizzo di tecnologia blockchain per casi d'uso specifici.

Middleware Provider – Scrypta fornisce il software necessario allo sviluppo di applicazioni Blockchain Oriented.

ASPETTO PRATICO

Esempio di funzionamento

Per comprendere il funzionamento del sistema, ci serviamo di un esempio pratico, immaginando che attraverso una dApp, un utente qualsiasi, mediante il suo cellulare, voglia inserire una fotografia all'interno della blockchain e che desideri che questa venga mantenuta permanentemente dall'infrastruttura.

Ecco i passaggi:

- 1) L'utente accede alla dApp attraverso un processo di autenticazione.
- 2) Il sistema fornisce all'utente un indirizzo pubblico sulla blockchain di Scrypta e le rispettive chiavi di accesso.
- 3) L'utente scatta la sua fotografia e procede con il processo di caricamento (immaginatelo come il caricamento di una foto su Whatsapp).
- 4) Il sistema a questo punto invia due distinti comandi al nodo di interfaccia IdA Node: il primo riguarda il caricamento del file su IPFS, mentre il secondo consente l'inserimento del riferimento di questa informazione (un identificativo univoco della foto) all'interno della blockchain.
- 5) L'utente attende i tempi tecnici affinché la blockchain processi la sua transazione (circa 2 minuti).
- 6) L'informazione e il file collegato (la fotografia) sono inserite per sempre all'interno della blockchain di Scrypta.

AMBITI APPLICATIVI

Alcuni esempi di utilizzo

Come oramai assodato, la blockchain ha avuto un impatto importante nel settore finanziario, con benefici evidenti in termini di velocità di processo dei dati, trasparenza, sicurezza, tuttavia questi benefici si possono applicare a moltissimi altri settori economici, produttivi e sociali, vale a dire in qualunque settore sul quale insistono molteplici intermediari. Ecco alcune aree potenziali di applicazione di Scrypta:

Filiera produttiva

La blockchain consente di creare delle filiere aperte in cui tutti gli attori, quali produttori di materie prime, imprese che si occupano di logistica e trasporti, imprese che operano sulle materie prime a vari livelli di trasformazione, aziende che lavorano su packaging e marketing e, infine i retail possono conferire dati e informazioni e controllare, con la massima trasparenza, i dati di tutti gli altri attori. I dati relativi a ciascun prodotto possono essere messi a beneficio del consumatore finale.

La nostra proposta tecnologica ha il potenziale per consentire non solo ai produttori, ma anche ai loro clienti, di entrare in un innovativo capitolo della tracciabilità nella catena di fornitura. La Blockchain di Scrypta può garantire un flusso informativo chiaro e scevro da irregolarità. E possiamo spingerci ad immaginare un prossimo futuro in cui una "scansione" dell'etichetta di un prodotto possa mostrare al cliente il percorso dalla sorgente al fruitore finale.

Industrial IoT (Internet of Things)

La Blockchain di Scrypta si candida al ruolo di applicazione chiave per l'Industrial IoT (Internet of Things). Può essere utilizzata infatti per tracciare miriadi di dispositivi collegati, consentendo l'elaborazione delle transazioni di dati che questi producono e il coordinamento tra i device fisici.

Questo approccio decentralizzato eliminerebbe i punti di guasto (failure) delle reti tradizionali, facilitando la creazione di un ecosistema sul quale potranno operare i dispositivi e i macchinari connessi.

La blockchain serve come un libro mastro pubblico per una massiccia quantità di dati e questo permetterebbe di bypassare l'utilizzo di un hub centrale per gestire e mediare la comunicazione tra i dispositivi. Gli algoritmi crittografici utilizzati da Scrypta, inoltre, permetterebbero di aumentare la tutela e la genuinità dei dati stessi.

Pubblica Amministrazione

L'architettura di Scrypta può cambiare radicalmente il sistema di relazioni tra i cittadini e la PA in ragione di una logica decentralizzata e distribuita, che porta a una maggiore trasparenza, a una maggiore sicurezza e accessibilità.

Si immagina l'utilizzo della blockchain nell'ambito della tenuta dei registri pubblici, nella conservazione documentale, identità digitali, pagamenti, riscossione delle imposte fino a meccanismi di votazione.

Copyright, brevetti e contratti

Grazie alla blockchain di Scrypta, è possibile l'inserimento di documenti come prove a sostegno durante diatribe legali che dimostrino inequivocabilmente la proprietà di un'opera o documento.

Due sono le caratteristiche che rendono Scrypta particolarmente rilevante per il sistema di certificazione: l'"hashing" e la "prova dell'esistenza"(Proof of Existence). L'hashing è un processo attraverso il quale un documento viene trasformato in un codice di lunghezza fissa che viene definito con un'impronta digitale. Ogni hash è unico.

Quanto alla "Proof of Existence", essa dimostra che un determinato hash esisteva in un determinato momento. Dimostrarne l'esistenza significa fornire la prova che un determinato documento esisteva in un momento fissato, questo processo viene definito "timestamping". Una opportunità questa ritenuta particolarmente interessante in tutti i processi che toccano il tema della proprietà intellettuale, dei brevetti e delle certificazioni.

Sanità

Gestire i dati medici dei pazienti attraverso la blockchain, permetterà di condividere informazioni sui pazienti in maniera sicura e veloce, e quindi aiuterebbe molto la medicina e la sanità a migliorare il servizio offerto, con la possibilità di avere sotto controllo l'intera cartella clinica di un paziente, e quindi di conoscere in anticipo la sua storia, in modo da somministrare cure migliori e in tempi più rapidi.

La blockchain è anche una risposta in termini di gestione di scenari complessi che riguardano la presenza e l'interazione tra sistemi sanitari interregionali, tra soggetti privati come possono essere i laboratori di analisi, le strutture della sanità privata o anche le assicurazioni.

La tecnologia blockchain di Scrypta può inoltre velocizzare le procedure di controllo e i meccanismi operativi delle strutture ospedaliere e può portare importantissime efficienze a livello di gestione documentale sicura.

E-commerce

Quattro i benefici della Blockchain di Scrypta nell'ambito del commercio elettronico:

1. *Lotta alla contraffazione*: le piattaforme di ecommerce possono verificare l'autenticità di ogni prodotto prima di esporlo al pubblico, a garanzia sia del cliente, sia della propria immagine.
2. *Ottimizzazione della Supply Chain*: come abbiamo visto nella sezione relativa alla filiera produttiva.
3. *Velocizzare i processi di pagamento*: che attualmente coinvolgono una pletera di attori sia lato cliente, sia lato merchant. Con la Blockchain si elimina la necessità di un ente centrale di autorizzazione, rendendo il processo di pagamento praticamente in real time.
4. *Sicurezza delle transazioni*: la natura immutabile e decentralizzata della blockchain rende di fatto impossibile alterare i dati e dunque elimina la possibilità di transazioni fraudolente.

Sicurezza Informatica

Con l'adozione di database basati su Scrypta è ipotizzabile una importante riduzione delle attività di hackeraggio, di manomissione e di intrusione nei database aziendali. Non solo i registri distribuiti al momento sono più sicuri rispetto a molti sistemi tradizionali, ma con la blockchain si elimina di fatto la necessità di interventi da parte di operatori, riducendo così i rischi legati all'errore umano.

Tracciabilità dei Rifiuti

In questo settore la Blockchain di Scrypta funzionerebbe come un vero e proprio sistema di verifica che permetterebbe di rilevare qualità, quantità del materiale e provenienza, al fine di tracciare tutto lo storico della filiera, facilitando il rapporto tra gli attori coinvolti in termini di affidabilità e sicurezza.

Inoltre la blockchain, sempre in relazione alla fase di gestione dei rifiuti, può essere utilizzata come strumento per incentivare comportamenti virtuosi dei cittadini.

Finanza e Banche

La Blockchain di Scrypta può aiutare le banche a fornire servizi più adeguati alle esigenze di imprese fortemente innovative e nello stesso tempo di disporre delle informazioni più precise sull'impresa cliente.

Assicurazioni

Gli assicuratori avrebbero nella Blockchain di Scrypta un'opportunità per ridurre i costi delle loro piattaforme di gestione, migliorare allo stesso tempo l'esperienza utente (customer experience) e sviluppare nuove soluzioni e opportunità attraverso un accesso ai dati migliorato.

Appendice I

I PARAMETRI DI BASE DI SCRYPTA

Coin Name LYRA	Ticker LYRA
Coin Type POS/MASTERNODE	Hashing Algorithm QUARK
Block Time 60 sec.	Block Size 1 MB
Max Supply 50,000,000	Premined 9,000,000
Reward Method SEE SAW MECHANISM	RPC & P2P ports 42223/42222

Appendice II

PIANO DI DISTRIBUZIONE DELLE RICOMPENSE

(per altezza di blocco)

Altezza di blocco	Premi per blocco	Supply (LYRA)	Giorni Aggregati
0 > 10	0	0	0,006 giorni
11 > 31	450000	9.000.000	0,01 giorni
32 > 499	0	9.000.000	0,32 giorni
500 > 750	2	9.005.000	1,75 giorni
751 > 173551	10	10.733.000	4 mesi
173552 > 691952	9	15.398.600	1,3 anni
691953 > 1210353	8,1	19.597.640	2,3 anni
1210354 > 2247154	6,5	26.316.104	4,3 anni
2247155 > 3283955	5,2	31.690.875,20	6,2 anni
3283956 > 5357556	3,1	38.140.600,64	10,2 anni
5351158 > 7431157	1,9	42.010.435,90	14,1 anni
7431158 > 14573108	1,1	50.000.000	27,7 anni

L'assegnazione del rapporto dei premi tra MN e PoS è bilanciata dinamicamente attraverso il meccanismo **SeeSaw** e muta in base a diversi fattori, in primis le quote delle monete totali bloccate sulla rete dai masternodes. L'assegnazione è prevista con un rapporto del 50/50 al raggiungimento di 500 MN in rete a fine 2019 (41,5% della Circulating Supply).

Appendice III - ROADMAP

Evento	Specifiche	Data
<i>Genesis Block</i>	Creazione e hardcoding del blocco ed avvio della blockchain.	21 dicembre
<i>Block Explorer</i>	Lancio del Registro Pubblico https://chainz.cryptoid.info/lyra/	22 dicembre
<i>Fase Genesi</i>	Contribuzione in forma privata e attivazione di 50 Masternode	01 gennaio 2019
<i>Apertura Canali Social e Forum</i>	Lancio dei canali ufficiali di Scrypta: BitcoinTalk/Discord/Telegram/Twitter	10 gennaio
<i>Rilascio Wallet Ufficiale v1.0.1</i>	Rilascio del codice ufficiale open source sulla piattaforma github	11 gennaio
<i>Light Paper (official)</i>	Pubblicazione di Scrypta Light Paper (documento sintetico)	12 gennaio
<i>Scrypta Website Beta</i>	Presentazione del sito ufficiale: www.scryptachain.org	13 gennaio
<i>Public Contribution Launch</i>	Disponibilità di n.100 masternode per i contributors (0,5 BTC a MN)	28 gennaio
<i>Whitepaper</i>	Rilascio White Paper ufficiale	28 gennaio
<i>Scrypta MN Bot</i>	Bot di monitoraggio masternode via Telegram/Discord	30 gennaio
<i>Exchange Listing</i>	LYRA Listing su www.mecatox.com	16 febbraio