2019

CRYPTO HIDE COIN

Decentralized Trustless

Whitepaper

WWW.CRYPTOHIDECOIN.ORG

ITALIANO

Contenuti

0. Prefazione

Questo documento è dedicato alla **blockchain** e alla **criptovaluta** denominata **Crypto Hide Coin**.

Crypto Hide Coin è una **criptovaluta decentralizzata** alla base di un **ecosistema blockchain** di **terza generazione**. Crypto Hide Coin è una criptovaluta avanzata concepita per community moderne proiettate alla crescita e allo sviluppo.

Le peculiarità sono:

- La piattaforma **non prevede costi** per lo *scambio di valore* tra gli utenti.
- Il sistema è interamente **esplorabile** ed è **espandibile** attraverso l' **Extended Chain,** che verrà introdotta in seguito.
- Implementa la tecnologia di **transazioni in tempo reale** (**Transaction Chain Ledger**)
- **Masternode trustless** progettati per un **ridotto impatto energetico** (**green-eco**)
- *Network interamente* e *costantemente sincronizzato*
- *Garanzia* delle transazioni basata sul consensus **Proof of Stake** (**PoS**).
- Il sistema è **Multilayer**
- Implementa il **social collaboration**
- Garantisce l' **e-voting**.

La base criptografica su cui si poggia è la **SHA-256** mentre il protocollo di riferimento è **CHPSv_x**.

Un sistema ricco di servizi di terze parti basati sullo scambio di valore equo.

1. Guida alla consultazione

Con il termine **Whitepaper** o **libro bianco** viene inteso un *documento utile a rappresentare in dettaglio la soluzione ad un problema*.

Questo è un **Whitepaper** e in quanto tale propone una soluzione ad un problema trasversale a diversi settori (finanziario, informatico, sociale, etc.).

La *prima parte* di questo documentazione si concentra sul problema, la necessità, la soluzione e il progetto mentre la *seconda* definisce i punti fondamentali del sistema (area tecnica).

Questo Whitepaper affronta il tema del mondo decentralizzato: **Blockchain**, **SmartContract**, **Criptovalute**, **Lending**, **ICO**, **IEO**.

Per la comprensione di questo documento NON è richiesta competenza tecnica.

Per una migliore comprensione è necessario avere una conoscenza essenziale del mondo della **blockchain** e delle **criptovalute** mentre per comprendere appieno ogni elemento del progetto è consigliabile approfondire questi temi.

Questo documento è stato redatto il 1 Settembre 2019 e si riferisce alla prima versione del Whitepaper.

E' possibile seguire gli aggiornamenti e le evoluzioni ai seguenti indirizzi:

- Sito ufficiale Crypto Hide Coin (https://www.cryptohidecoin.org)
- Github (https://github.com/CryptoHideCoin)

Le **specifiche tecniche** del protocollo sono disponibili all'interno del **Yellowpaper**.

2. Esclusione della responsabilità

Questo documento può contenere **errori di traduzione**, di **contenuto** o **imprecisioni**. Proseguendo con la lettura si accetta la possibilità che alcune informazioni possano non essere precise.

Le citazioni contenute all'interno di questo documento si riferiscono a prodotti di pubblico dominio o a personaggi pubblici.

Qualsiasi **imprecisione**, **omissione** o **errore** può essere segnalata scrivendo ad info@cryptohidecoin.org

3. Lo scenario attuale

3.1 In premessa

Questo decennio ha prodotto, in campo informatico, due grandi scoperte tecnologiche: la **blockchain** e le **criptovalute**, elementi in cui sono numerosi i campi d'applicazione e che trovano quotidianamente spazio nelle nostre vite.

Sebbene essi siano dei concetti nuovi, grazie alla diffusione crescente sulla stampa, in televisione e su Internet, essi diventano sempre più familiari al grande pubblico.

3.2 Andamento di mercato

Di seguito è riportata la capitalizzazione media del segmento delle **criptovalute** distinta per anno:

Anno	Capitalizzazione (in dollari
2009	394.200
2010	7 milioni
2011	70 milioni
2012	500 milioni
2013	1 miliardo
2014	8 miliardi
2015	5 miliardi
2016	7 miliardi
2018	785 miliardi
2019	128 miliardi

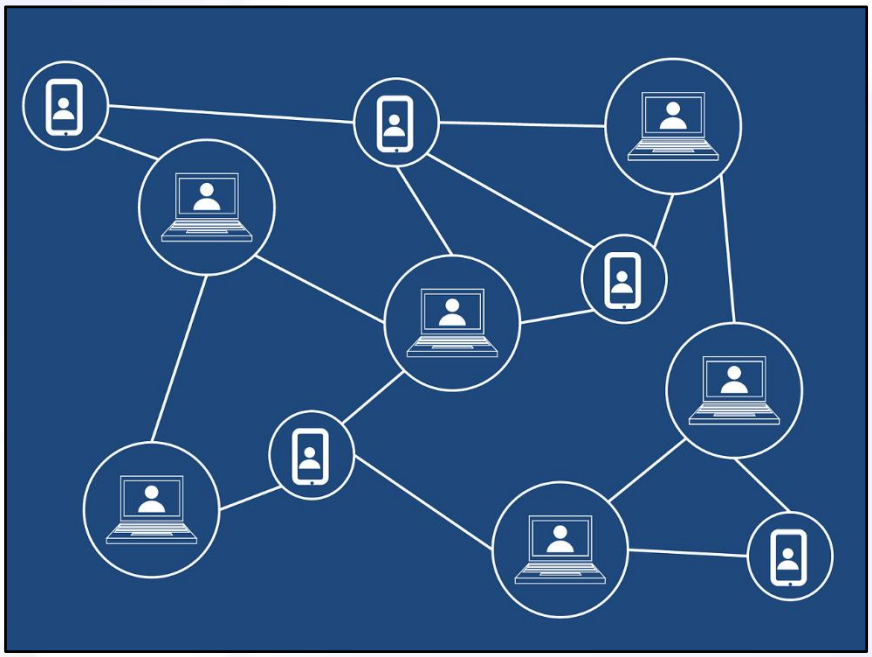
La tabella illustra il crescente interesse del mercato per il settore.

Il numero delle **criptovalute** è cresciuto in pochi anni da un ridotto numero ad un numero consistente.

3.3 La nostra ipotesi

Sia gli **sviluppi tecnici**, **normativi** che l'**apprezzamento degli utenti** portano a pensare che in futuro andremo incontro ad un'adozione di massa di **cripto valute** e **servizi blockchain**.

Per questa ragione, abbiamo elaborato un modello di blockchain polifunzionale (basato su una moneta nativa) atto a risolvere le numerose necessità che esporremo in questo documento. Questo modello è pensato per consentire a piccole realtà e privati, di trarre vantaggi e poter offrire le proprie soluzioni decentralizzate.



4. Il problema

Il settore fintech, ad oggi, ha conosciuto tre stadi evolutivi.

La *prima generazione* ha dato il via al settore ed ha rappresentato la vera e propria essenza delle cripto valute: solo scambio di valore.
La *seconda generazione* è stata caratterizzata dall'aver introdotto il concetto di **smart contract**.
Infine, l'ultima generazione di cripto valute presentano una **migliore articolazione**, **maggiore efficienza** e una **strutturazione multi-livello** (sidechain).

Nonostante gli sforzi effettuati dalle numerose community di altcoin, ad oggi rileviamo numerosi problemi con soluzioni più o meno improvvisate.

Tra questi rileviamo:

- Solo un numero modesto di blockchain offre **tempi accettabili** di conferma delle transazioni.
- Troppe blockchain sono **dispendiose dal punto di vista energetico**.
- E' ancora alto il divario tra i **costi delle transazioni dei servizi** in criptovaluta e i servizi tradizionali.
- Le blockchain/criptovalute attuali NON consentono ancora un adeguato **livello di privacy**; le uniche che affrontano il problema non sono inquadrabili con nessuno degli standard in materia di antiriciclaggio.
- Blockchain ghettizzate alla risoluzione di un problema specifico

Crypto Hide Coin Decentralized Trustless affronta e risolve i citati problemi.
La batteria di servizi integrati la qualifica come un vero e proprio **Social Business Network** basato sul rispetto della riservatezza dei dati unito alla trasparenza e alla controllabilità delle transazioni.

5. Il progetto

Crypto Hide Coin Decentralized Trustless è una **piattaforma** interamente *decentralizzata* basata su un'infrastruttura **peer-to-peer**.

Attraverso l'uso combinato tra **registro pubblico distribuito** e relazione *fiduciaria* (**gatechain**) è consentito ai *membri della community* piena libertà di **scelta del grado di riservatezza** o di **trasparenza** da adoperare nello **scambio di informazioni personali** e/o **valore**.

Questo sistema supera l'*annoso* ed *ambizioso* problema di porre sullo stesso piano *trasparenza* e *riservatezza*: il perfetto connubio tra *pubblico* e *privato*!

Crypto Hide Coin Decentralized Trustless si pone come ecosistema completo di *servizi utili*, in *continua espansione*, a forte *impatto sociale*, *innovativi* e perfettamente *integrati* tra di loro.

Tra le caratteristiche di assoluto rilievo troviamo:

- **Minimo impatto energetico** (no Proof of work)
- **Transazioni in tempo reale** (**Transaction Chain**)
- **Nessun costo previsto per le operazioni di scambio di valore**

6. La Soluzione

Per risolvere le citate problematiche è stata progettato una nuova tipologia di **registro pubblico decentralizzato** denominato **Transaction Chain Ledger**.

Le caratteristiche di questo strumento sono:

- **Transazioni immediate**
- **Smart-contract predefiniti**
- Annotazione delle **informazioni polimorfiche**
- Integrazione con **side chain**
- Consenso basato su **Proof Of Stake**
- Certificazioni basate su **Proof Of Identity**
- **Scambio di valore** tra soggetti singoli o multipli con quote paritarie o diversificate
- **Transazioni a firma singola o multipla e/o differita**
- **Registrazione di domini mono e multilivello**
- **Registrazione di indirizzi ad aree personali**
- **Wallet root only read**, **cumulativi**, **permissioned**, **cointestati** a **firma congiunta e disgiunta**

I *fondatori* e il *team di sviluppo* di **Crypto Hide Coin** hanno sottoscritto un impegno con la propria comunità: rendere integrati, facili da usare ed accessibili tecnologie e servizi utili, importanti ma di base complessi.

7. Ambiti di applicazione

Gli ambiti di applicazione di **Crypto Hide Coin** sono:

- **Trasferimento di valore** trustless
- **Pagamenti**, **custodia** e **scambio di valore** fiduciaria su architettura decentralizzata
- **Certificazione** professionale
- **e-Voting** / **sondaggi**
- **Accreditamento previsionale** e/o **analitico**
- Automazione del processo di **riscatto assicurativo** / scommesse, **raccolta fondi** e **garanzie**
- **Annotazione di proprietà**, **registrazione di copyright** e **trasferimento di proprietà**
- **Gestione abbonamenti**
- **Gestione sottoscrizioni**
- **Gestione contratti** tra le parti
- **Comunicazione certificata** e/o privata
- **Tracciatura**
- **Annotazione di testamenti** ed eredità
- **Donazioni** e **beneficienza**
- **Raccolta fondi**
- **Sviluppo di progetti**
- **Exchange decentralizzato**
- **Posizioni offerte a garanzia** o **lending**
- **Pubblicazione di offerte**
- **Scambio e condivisione** privata di files

8. Specifiche tecniche della moneta

Di seguito le specifiche tecniche di **Crypto Hide Coin Decentralized Trustless**:

Caratteristica	Valore
Blockchain Name	Crypto Hide Coin Decentralized Trustless
Short Name	CHCS
Type	Coin
Blocktime	Realtime
Currency Symbol	§
Algorithm	SHA-256
Protocol	CHPSv_x
Consensus Mode	Proof of Stake (POS)
Total Supply	1.300.000.000
Premined	250.000.000
Reward per day	100.000
RPC & P2P Ports	21212

9. Storia di questo progetto

Crypto Hide Coin Decentralized Trustless nasce come naturale evoluzione del progetto **Crypto Hide Coin**.

Crypto Hide Coin è un progetto nato nel 2011 per opera di tre ingegneri vietnamiti.
Esso è un coin *Privacy Oriented*, *Decentralized Trusted*, basato sul *Proof Of Identity*.

10. Roadmap

Il progetto prevede un lungo termine per essere completamente dispiegato e ultimare una diffusione capillare.

Di seguito il riepilogo suddiviso per anno:

Anno	Obiettivo
2019	Funzionalità Coin Core utile allo scambio del valore
2020	Presentazione al coin market Funzione di Pilot Reward Servizi di notariato Blockchain Servizi enterprise Decentralize Price List Co-Signature e Multiple-signature
2021	Servizio di exchange decentralizzato Funzionalità avanzate
2022	Servizio di exchange integrato
2023	Servizi per lo sviluppo di progetti collaterali
2024	Sistema monetario a valore unico Sistema monetario personalizzato
2025	Integrazione per il sistema di finanziario fiduciario
2026	Social Finance Network
2027	Integrazione con servizi web a valore aggiunto
2028	Servizi per la diffusione extraweb

Articolo 1 - Definizione di Crypto Hide Coin

Crypto Hide Coin è un'infrastruttura **Peer-to-Peer** *controllata* (*permissioned*), *decentralizzata*, *aperta*, *trasparente*, *scalabile*, *esplorabile* e *sicura*.

Le informazioni contenute sono state garantite da tutti i *peer* attivi e sono integre in ogni sua parte. Chiunque può verificare la veriticità delle informazioni contenute.

Essa si basa sul protocollo **CHPSv_x**.

La *mutua cooperazione* dei *peer* aderenti al circuito consentono l'espletazione dei servizi indicati di seguito:

- **Scambio di valore**
- **Riconoscimento**
- **Identificazione**
- **Notariato**
- **Espressione di consenso**
- **Sottoscrizione abbonamenti**
- **Annotazione**
- **Tracciatura**
- **Recapito messaggi privati**
- **Controllo della gestione fiduciaria**
- **Certificazione**
- **E-Voting**

Ogni servizio viene svolto in *concorrenza* (**Trustless Mode**) all'interno del *network*.

Articolo 2 – Principio di funzionamento

L'intera **piattaforma** offre i servizi citati all' articolo 1 attraverso la combinazione di una *rete decentralizzata* e lo *scambio di messaggi* tra le parti. Le parti interessate allo scambio di messaggi sono i peer e sistemi client.

I **messaggi** vengono utilizzati per ogni tipo di attività: sia per le **richieste**, sia per l'ottenimento delle **risposte**, che per la diramazione di **aggiornamenti**.

Ogni *peer* è **autoconsistente** e contiene una **copia fedele** (verificata) di tutte le *informazioni*, nonchè una versione integra ed aggiornata di un **Registro Pubblico Decentralizzato** denominato **Transaction Chain Ledger**.

Ogni *peer*, una volta ricevuta una richiesta attraverso un messaggio ha l'obbligo di effettuare una **verifica formale**. In caso di esito positivo, lo stesso dovrà essere propagato in rete. Qualora anche la verifica integrale dovesse essere positiva sarà proposto l'aggiornamento del registro pubblico suddetto.

Articolo 3 – Il Registro Pubblico Decentralizzato

Ogni copia del *Registro Pubblico Decentralizzato* dovrà contenere l'*annotazione di ogni richiesta* utile alla *variazione* dello *stato della Blockchain* e la *trascrizioni terze* a valore aggiunto.

Qualsiasi proposta di richiesta di ampliamento del *registro* dovrà pervenire da una *maggioranza qualificata* dei *peer* del network: i due terzi del totale del valore posto a garanzia.

La procedura di *aggiornamento/estensione* del *registro* avviene attraverso un processo denominato consensus o validazione.

Esso si basa sulla *convergenza* dei *consensi* dei *peer* sulle singole proposte (e non su blocchi) di aggiornamento.

Ogni *trascrizione* dovrà essere accompagnata dalle informazioni che garantiscano l'*immutabilità* di tale *scrittura* (valore *hash* risultante).

Articolo 4 – I Wallet

Un **Wallet** o **portafoglio elettronico** è rappresentato da un software (programma) o servizio web che consente, attraverso il collegamento alla rete **peer-2-peer**, utili a *conservare* e *gestire* **criptovalute**.

Articolo 5 – Rete sincronizzata

Ogni *peer* ammesso al circuito **Crypto Hide Coin** ed ha i seguenti oneri:

1. **Verificare l'integrità** della Transaction Chain
2. Gestire le **richieste provenienti dai client** (Wallet)
3. Gestire le **richieste di ammissione** provenienti da potenziali nuovi peer
4. Gestire le **richieste inoltrate** da altri *peer*
5. **Validare formalmente** le richieste ricevute
6. **Propagare** al network la richiesta validata
7. **Aggiornare la** Transaction Chain con le richieste valide
8. **Propagare la** Transaction Chain locale al network

Ogni *peer* ha il **diritto di ricevere**:

1. I **feedback** provenienti dagli altri *peer* a seguito delle richieste inoltrate
2. Avere **conferma** dagli altri *peer* delle operazioni svolte

Ogni *peer* offre, a garanzia della sua *integrità*, il blocco del valore associato al **wallet**. Esso sarà confiscato dal network (e redistribuito agli stakers) in caso di palese tentativo di *contraffazione/alterazione* della **Transaction Chain**.

Il *Peer*, per le attività espletate, riceverà una **compenso** proporzionale al *valore posto a garanzia*.

Ogni *peer* sarà sempre aggiornato e sincronizzato con le operazioni annotate da tutti gli altri *peer*.

Tra i *peer* ammessi alla rete è possibile distinguere:

- Gli **Staker** o **Masternode** offrono servizi di rete in cambio di un numero di monete proporzionale a quanto offerto in garanzia
- I **Checker** si limitano ad effettuare il controllo dell'integrità della Transaction Chain in cambio di monete (non partecipano al consensus). Tra le altre funzioni svolte da questo tipo di peer è anche presente la condivisione dei file della Transaction Chain
- I **Guest Node** ricevono passivamente feedback degli aggiornamenti della Transaction Chain senza la partecipazione (e senza essere ricompensati) ai servizi del network

Articolo 6 – Il peer di Genesis

Il *primo avvio* del network sarà effettuato da uno speciale peer denominato **Genesis**.

Esso è contraddistinto dalle seguenti semplificazioni rispetto gli altri nodi della rete:

- *Nessun valore* di saldo richiesto per l'ammissione al circuito
- *Nessuna garanzia* necessaria richiesta a cauzione delle operazioni svolte

Tale assenza di requisiti sarà ritenuta ammissibile al solo primo avvio della rete.

Articolo 7 – Il consenso basato sul maggiore interesse

Ogni *peer*, che svolge l'attività di controllo e di gestione attiva della Transaction Chain, è obbligato ad *impegnare* dei fondi, come descritto all'interno dell'articolo 5.
La *quota proporzionale* dei *fondi impegnati* rappresenta il "peso" del voto esercitato per ogni *transazione validata*.

Articolo 8 – Network basato su una rete permissioned

Ogni *peer* appartenente al network deve essere precedentemente accettato dal network stesso.

Ogni *peer*, per essere ammesso al circuito, deve **disporre dei seguenti requisiti**:

1. Essere associato ad un *indirizzo di un wallet*
2. Avere un **wallet con saldo maggiore di zero** (ad eccezione del Nodo di genesis)
3. Presentare *domanda formalmente valida*
4. Offrire a **garanzia l'intero saldo**
5. Supportare la **versione minima** del protocollo
6. Aver verificato il **ledger** della Transaction Chain pubblicato dal network
7. Accettare la Transaction Chain attiva sul network

Articolo 9 – Contratto di scambio valore

La Transaction Chain, offre un servizio base per lo **scambio di valore** tra le parti.

Esso si concretizza tramite monete detenute e gestibili da *indirizzi di portafogli* (**wallet**).

Le regole e le modalità di funzionamento del conio sono indicate nel **contratto di valore** marcato sulla prime iscrizioni della Transaction Chain.

Articolo 10 – Proposizione aggiornamento Transaction Chain

Il registro della Transaction Chain può essere aggiornato solamente a seguito di un'*approvazione qualificata* dai peer che hanno posto maggiore valore a garanzia.

Dal momento della ricezione della richiesta è necessario svolgere una verifica completa; essa determinerà l'**accoglimento** o il **rigetto** della richiesta stessa.

Il *peer *che ha *raccolto*, *processato* ed *inoltrato* la richiesta assume il nome di **peer master**.

In caso di accoglimento, all'intero network sarà inoltrato un messaggio accompagnatorio dell'originale con la proposta di aggiornamento della Transaction Chain.

Nel caso in cui la richiesta non disponga degli estremi sufficienti per l'accoglimento, sarà in tutti i casi rigirata al *network* con le *motivazioni del rigetto*.

Alla ricezione di tutti i feedback si potrà effettuare il conteggio dei consensi e quindi procedere con l'**aggiornamento del registro**: la stessa azione sarà effettuata dagli altri peer.

In assenza di messaggi elaborati in contemporanea dalla rete, sarà onere del peer master l'invio di un messaggio di consolidamento della Transaction Chain.

Crypto Hide Coin non è denaro

Crypto Hide Coin non è un investimento finanziario

CHI SOSTIENE QUESTE TESI SI SBAGLIA

Crypto Hide Coin è uno strumento informatico

Crypto Hide Coin è un progetto innovativo

Evitare di confondere tecnologia con strumenti finanziari: sono due cose diverse!