MONETA DUCATUS

LIBRO BIANCO

DUCATUS

DUCATUS

CHE COS'È DUCATUS?

Ducatus fornisce la più robusta combinazione al mondo di infrastruttura di criptovaluta con un sistema di distribuzione network marketing. L'abile uso del potere di distribuzione di un sistema di network marketing attentamente strutturato con la scalabilità, sicurezza, e durevolezza di una criptovaluta progettata in modo robusto dà alle tue monete Ducatus reale e duraturo valore.

I membri di Swissmine.club possono comprare e vendere crediti di creazione di Ducatus e monete digitali dal sito web Swissmine.club. Le monete possono essere immagazzinate in modo sicuro in un portafoglio digitale su un telefono, computer desktop, o sul sito web Swissmine.club. Quando un membro vuole effettuare un acquisto usando le proprie monete Ducatus, fa semplicemente un trasferimento dal portafoglio di loro scelta al venditore. Questo funzionerà non solo per gli acquisti online ma in futuro anche per i punti di vendita al dettaglio.

COME FUNZIONA

Le criptovalute si basano su un libro mastro distribuito detto "blockchain". Questo libro mastro tiene traccia di tutte le transazioni tra portafogli digitali nella rete. I portafogli sono applicazioni che sono eseguite su telefoni di membri del club e su computer desktop. Quando un membro vuole inviare delle monete Ducatus da un portafoglio ad un altro, inserisce l'indirizzo pubblico del ricevente e l'importo. La rete di tutti i portafogli membri allora unisce le forze per verificare e validare la transazione, che, una volta verificata, è scritta sul libro mastro condiviso.

I blockchain sono la salsa segreta che fa funzionare le criptovalute. Contengono una base dati di tutte le transazioni che hanno avuto luogo coinvolgendo quella criptovaluta. Ci si riferisce ad esso come blockchain perché è costituito da una serie di blocchi ciascuno dei quali è un insieme di transizioni nel libro mastro che hanno luogo durante un breve periodo di tempo. Al fine di generare il prossimo blocco, i portafogli competono per risolvere un problema crittografico impegnativo che scoprono solo quando il precedente blocco è completato. Quando un portafoglio pensa di avere risolto il problema, gli altri portafogli lavorano per verificare che sia veramente corretto. Una volta che un numero sufficiente di portafogli abbiano confermato la correttezza del blocco, questo è aggiunto al blockchain di tutti i portafogli. Questo processo è chiamato mining.

Mentre il blocco è stato creato, I portafogli si comunicano le transazioni l'un l'altro. Una transazione è semplicemente un trasferimento di monete di criptovaluta da un portafoglio ad un altro, basato sui loro indirizzi pubblici. Assumendo che un numero sufficiente di portafogli sia d'accordo che una transizione sia stata fatta durante il processo di mining, queste transazioni sono aggiunte al libro mastro nel blockchain, a questo punto tutti i portafogli nella rete riconoscono che il trasferimento di monete ha avuto luogo. Siccome i tuoi portafogli partecipano all'operazione di mining e creano blocchi con successo, riceveranno un certo numero di piccoli pagamenti in monete Ducatus da altri membri nella forma di onorari. I portafogli eseguiti sui computer desktop possono ricevere ricompense più significative dal momento che hanno una più grande capacità di elaborazione dei portafogli sui telefoni.

I portafogli contengono un insieme detto “keyring” di indirizzi pubblici che danno loro modo di identificarsi pubblicamente nel libro mastro. Per ogni indirizzo pubblico, un portafoglio ha una corrispondente chiave segreta o privata a cui solo i membri hanno accesso. Un portafoglio può generare indirizzi pubblici multipli al fine di distinguere tra diverse ragioni per eseguire transazioni con le monete. Questo è qualcosa di simile alle cifre aggiuntive in un numero di conto bancario che ti permette di sapere se è riferito al conto corrente o al conto di risparmio. Se un membro di Swissmine.club vuole usare diverse piattaforme, per esempio, una sul loro iPhone e una sul sito web, dovrà creare un portafoglio e un indirizzo per ciascuna piattaforma. I membri saranno facilmente in grado di trasferire monete tra i loro portafogli usando la rete di monete Ducatus.

Portafoglio Ducatus

Fare un acquisto con una criptovaluta è facile quanto usare una carta di credito, ma il modo in cui il libro mastro funziona significa che il processo può essere percepito come un po’ a rovescio all’inizio. I venditori che accettano monete Ducatus hanno dei propri portafogli che accettano monete Ducatus per gli acquisti. Quando un membro del club vuole fare un acquisto da un negozio, invia le sue monete all’indirizzo che il negozio gli dà e riempie il proprio indirizzo pubblico. Il membro dirà alla propria applicazione portafoglio di inviare la cifra corretta all’indirizzo, e poi la rete di moneta Ducatus si incarica di completare la transazione. Così, invece di mandare ad un venditore un codice come faresti con un numero di carta di credito, il venditore ti dà un codice da scrivere nel tuo portafoglio.

Dal momento che tutti I portafogli nella rete funzionano insieme per creare un libro mastro senza bisogno di connettersi a Swissmine.club, i membri sono in grado di usare le loro monete fino a che ci sono portafogli connessi a internet. Questo significa che ogni venditore che supporta le monete Ducatus può accettarle per sempre. Il libro mastro è distribuito tra tutti i portafogli, così ogni membro può facilmente vedere tutte le transazioni validate che sono state fatte sulla rete di monete Ducatus. Non occorre preoccuparsi che una terza parte come Swissmine tracci il tuo

credito di club – è tutto lì per tutti da vedere ed è crittograficamente e permanentemente messo in sicurezza.

TECNOLOGIA ALTERNATIVA A BITCOIN

A Ducatus usiamo un algoritmo industriale standard e la tecnologia blockchain per fornire un esperienza sicura e affidabile. Di conseguenza, abbiamo deciso di seguire le migliori, collaudate e verificate pratiche industriali per creare una criptomoneta alternativa al Bitcoin che è creata sulla base del codice sottostante al Bitcoin. Abbiamo creato un nuovo codice sorgente a partire dal codice open source dei portafogli Bitcoin e modificato i parametri della rete per creare una nuova moneta, la moneta Ducatus, con caratteristiche che crediamo funzioneranno meglio per i membri Swissmine.club. Il nuovo codice è una variante di un codice esistente che lo rende distinto dalle versioni precedenti. In questo caso essersi basati sul codice Bitcoin ci permette di creare una moneta che usa tutte le migliori caratteristiche del Bitcoin e omette o corregge quelle caratteristiche che è stato provato avere dei problemi o delle debolezze.

Uno dei più importanti cambiamenti che abbiamo fatto ai parametri standard Bitcoin è che abbiamo modificato il tempo necessario per il processo di mining dei blocchi. I blocchi Bitcoin impiegano in media 10 minuti per essere creati, periodo che è abbastanza lungo per le applicazioni come il commercio elettronico, per non parlare della vendita di articoli in un punto di vendita come un ristorante o un negozio (si immagini che il commesso di un negozio ti chieda di aspettare mentre elabora i dati della la tua carta di credito ... e ci vogliano 10 minuti o più per restituirtela!).

Dal momento che la maggior parte del codice originale provato e verificato è conservata, basarsi su un codice esistente è di gran lunga più stabile e sicuro che svilupparne indipendentemente uno nuovo (e così non verificato) per una nuova moneta. La comunità di sicurezza informatica ha un detto “non cercare di scrivere un codice crittografico del tutto nuovo”. In quasi tutti i principali casi dove un prodotto crittografico è stato compromesso ciò è avvenuto perché lo sviluppatore non ha eseguito verifiche indipendenti degli algoritmi crittografici usati nel proprio prodotto. Usare il Bitcoin come base per la nostra tecnologia significa che Ducatus beneficia di tutto il duro lavoro e delle analisi che sono già state fatte sul Sistema Bitcoin. Abbiamo ingaggiato i migliori esperti in sicurezza informatica per assicurare che il nostro nuovo codice sia anche molto sicuro, ma basandoci sul codice Bitcoin abbiamo già costruito sulle fondamenta della più solida criptovaluta del mondo.

Un altro principale beneficio di basarci sul codice Bitcoin che i venditori associati sono in grado molto più facilmente di adottare la moneta Ducatus. Ci sono molte librerie di codici esistenti che permettono ai siti di commercio elettronico di adottare Bitcoin su una base collega e usa, e dal momento che stiamo usando un’interfaccia di programmazione di applicazione quasi identica, i negozi web e gli scambi di criptovaluta potranno molto facilmente essere adattati per l’uso con i Ducatus. Dove in modo appropriato lavoreremo coi venditori e con la comunità di sviluppo di software non proprietario allo scopo di assicurare che le librerie pertinenti continueranno ad essere compatibili con Ducatus negli anni a venire.

CREARE UN PORTAFOGLIO

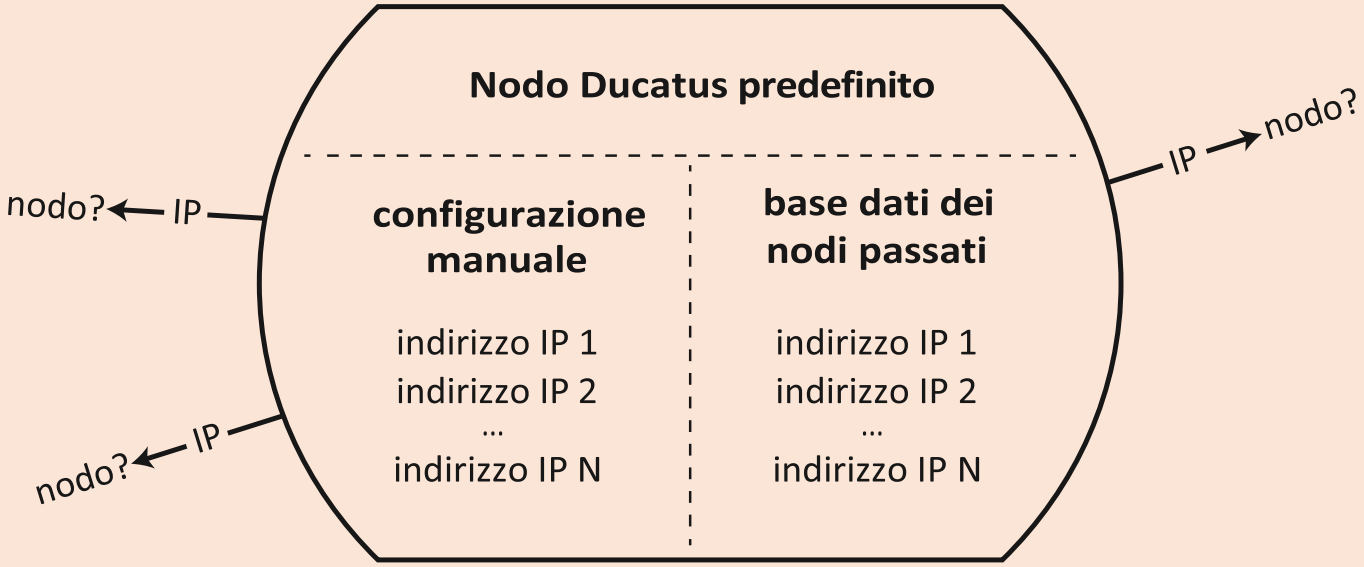
Swissmine.club fornirà mettendo a disposizione dei server internet dei portafogli web che i membri potranno usare per eseguire le transazioni con le monete Ducatus. Per i membri che vogliono la convenienza di avere e usare un portafoglio facilmente, offriremo applicazioni per iOS e Android. Gli utenti più avanzati e i membri che sono interessati a ricevere remunerazioni per il processo di mining dei blocchi possono scegliere di usare un portafoglio su un computer desktop, che sarà offerto per Windows, OS X, e Linux. Ciascuno di questi portafogli può unirsi alla rete delle monete Ducatus e inviare e ricevere monete.

Un membro che desidera usare un'applicazione portafoglio inizierà semplicemente scaricandola e installandola sul proprio dispositivo. Quando il portafoglio inizializzerà se stesso creerà una chiave privata e anche un indirizzo pubblico a cui ricevere le monete. L'utente può in seguito aggiungere più chiavi al proprio portafoglio come desidera. Per un membro è una buona idea creare una copia delle proprie chiavi private – se le perde, né lui né nessun altro sarà in grado di accedere ai contenuti del portafoglio. La nostra raccomandazione per i nostri membri per salvare le chiavi private è di stamparle e conservare la copia cartacea in luoghi diversi, in un luogo sicuro a casa propria e idealmente anche in una cassetta di sicurezza.

CONNESSIONE ALLA RETE

Uno dei portafogli è installato con le chiavi e gli indirizzi, è ora di connettersi alla rete delle monete Ducatus. Questa rete è costituita di tutti i portafogli Ducatus che sono connessi a internet – può essere vista come uno strato virtuale sulla rete internet. Questa tecnologia è simile a quella delle reti peer-to-peer che sono usate per applicazioni come BitTorrent.

I portafogli si trovano l'un l'altro attraverso un processo di individuazione dei nodi della rete. Un portafoglio appena creato che è connesso ad internet per la prima volta, userà il sistema dei nomi di dominio per cercare un server portafoglio Ducatus che contiene una lista di portafogli attivi. Ogni portafoglio mantiene una propria lista di nodi della rete, e la condividerà con gli altri portafogli attivi. Dopo che un portafoglio si è connesso la prima volta si riferirà prima alla propria lista salvata di nodi portafogli a cui si è connesso con successo in passato. C'è anche l'opzione di aggiungere manualmente l'indirizzo IP dei portafogli nel portafoglio Ducatus nel caso in cui nessuno di questi approcci abbia successo.



Individuazione dei nodi

LE TUE PRIME MONETE

Come membro di Swissmine.club otterrai le tue prime monete dal sito web Swissmine.club attraverso l'acquisto e la successive conversione di crediti di mining. Quindi puoi associare un indirizzo pubblico del portafoglio al tuo profilo di adesione sul sito web. In quel modo Swissmine saprà dove inviare le tue monete.

Una volta che il tuo profilo è impostato, puoi semplicemente cliccare per inviare monete al tuo portafoglio. Swissmine userà poi il suo portafoglio per iniziare una transazione sul blockchain Ducatus. I nodi portafoglio sulla rete eseguiranno la procedura di mine di un bocco, e poi quella transazione sarà aggiunta al libro mastro. A quel punto il tuo portafoglio riconoscerà che le tue monete Ducatus sono state aggiunte.

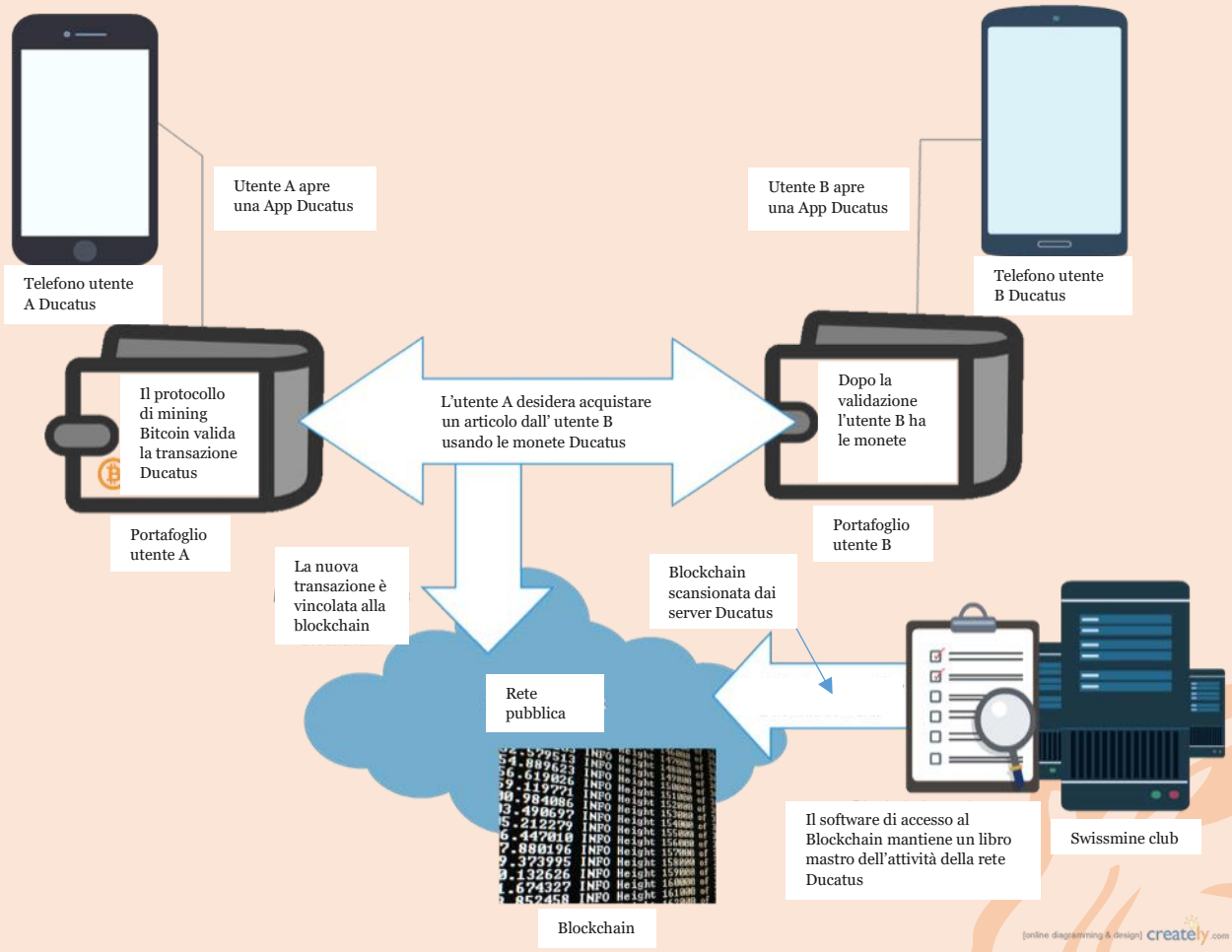
ESEGUIRE UNA TRANSAZIONE

A questo punto, le tue monete sono in tuo possesso e dipende da te che cosa vuoi farne. Puoi volere fare un acquisto da uno dei nostri venditori associati. Per fare questo useresti il loro negozio web online come ogni altro sito di commercio elettronico e quando esegui il pagamento semplicemente selezioneresti Ducatus come tuo metodo di pagamento.

A questo punto, i modi di procedere del venditore possono variare da un negozio all'altro, ma saranno qualcosa del genere: primo, il venditore usa il suo portafoglio per generare un indirizzo pubblico unico per la tua transazione, poi condivide quell'indirizzo pubblico con te e dichiara la cifra che ti chiederà di pagare, a quel punto, se stai usando un portafoglio su un computer desktop, puoi semplicemente copiare e incollare l'indirizzo nel tuo portafoglio e iniziare la

transazione. Molti venditori ti daranno anche l'indirizzo del loro portafoglio come un codice QR così che tu possa facilmente scansionarlo con l'applicazione portafoglio sul tuo telefono o tablet senza doverlo immettere manualmente.

Una volta che hai inizializzato il processo di pagamento, il venditore eseguirà la scansione del blockchain Ducatus per la transazione. Una volta che è stato trasferito al libro mastro e validato da un numero sufficiente di nodi delle rete, il venditore approverà il tuo pagamento e continua il processo proprio come farebbe se tu usassi una qualsiasi altra valuta.



MINING DEI BLOCCHI

Se stai eseguendo un portafoglio su computer desktop allora una volta che ha stabilito delle connessioni peer-to-peer con altri portafogli, è pronto per aiutare il processo di mine di alcuni blocchi e guadagnare la remunerazione per la transazione. Come utente hai bisogno di fare molto poco per abilitare questo – fintanto che la tua macchina è accesa e connessa, e se il processo di mining è abilitato, il portafoglio eseguirà il mining in background con ogni risorsa computazionale che è disponibile sulla tua macchina.

Che cos'è il mining, effettivamente? Ogni blocco nella blockchain Ducatus deve essere validato con un hash crittografico, algoritmo matematico che trasforma dei dati in una stringa binaria di dimensione fissa chiamata valore di hash. Questo hash è ottenuto matematicamente con la combinazione di tutti i blocchi precedenti hash con tutte le transazioni in corso che devono essere validate. La creazione di un hash è una operazione a senso unico, così è crittograficamente impegnativo trovare qual è quello nuovo; cioè hai bisogno di elaborare un gran numero di calcoli complessi per trovare la risposta. Tutti quelli che eseguono il mining lavorano eseguendo calcoli per trovare l'hash, e quando qualcuno annuncia di averlo trovato, gli altri possono velocemente verificarlo e validare la soluzione. Con un numero sufficiente di validazioni quel blocco è quindi aggiunto al blockchain distribuito Ducatus che è riconosciuto da tutti i portafogli e poi non può essere cambiato. Questo approccio risolutivo per validare tutte le transazioni Ducatus è usato ad un ritmo costante.

RECUPERO DEL FONDO

Fintanto che un membro ha creato un documento o ha salvato elettronicamente le sue chiavi private sarà sempre in grado di accedere alle proprie monete sul blockchain Ducatus, non importa cosa accade alla loro applicazione portafoglio, computer, o telefono. Questo perché le monete non sono realmente immagazzinate nel portafoglio – il loro deposito nel portafoglio è registrato nel libro mastro sul blockchain. Così se qualcosa va storto, tutto quello che i membri hanno bisogno di fare è scaricare la applicazione portafoglio e fornirle le chiavi private che ha salvato. Il portafoglio verificherà allora le sue chiavi rispetto agli indirizzi nella blockchain e poi avrà automaticamente accesso alle sue monete Ducatus di nuovo e saprà quanto valore è associato a ciascuna chiave.

MINING ANTICIPATO

Ducatus è insolita tra le monete alternative al Bitcoin perché il mining delle nostre monete è fatto anticipatamente. Storicamente, la maggior parte delle monete hanno usato il mining dei blocchi come un modo di fornire una ricompensa per il processo di mining di nuovi blocchi e la costruzione della blockchain. Usando la strategia Ducatus comunque, chi esegue il mining riceverà delle ricompense nella forma di una provvigione di transazione, ma invece inizieremo con un insieme di monete Ducatus e le distribuiremo ai nostri membri attraverso la nostra rete di marketing e il sistema di compensi associato per assicurarne una rapida ed estesa adozione in tutto il mondo.

GESTIONE DELLE SCORTE

Mentre abbiamo fatto i Ducatus i più decentralizzati e distribuiti possibile, ci sono ancora alcune considerazioni riguardo alla gestione delle scorte delle monete con mining fatto in anticipo. Fortunatamente, il trattamento di grandi portafogli è una sfida conosciuta nell'industria delle criptovalute e l'industria si è evoluta per sostenere equamente un processo sicuro e robusto.
Gli scambi di criptovaluta affrontano problemi simili a quelli che hanno molti membri che si scambiano le monete tra di loro. Quando un utente ha delle monete da scambiare per convertirle tra diverse valute le monete sono temporaneamente tenute nel portafoglio del

cambiavalute. Questo rende lo scambio un bersaglio allettante per gli avversari. Sono state sviluppate le migliori pratiche per assicurare la sicurezza del portafoglio per i cambiavalute e per sistemi come Ducatus. Il problema non è solo tecnico ma di seguire un'affidabile politica di sicurezza. La più grande minaccia ad ogni azienda che tiene significativi volumi di monete digitali è che chi eseguirà un attacco comprometterà la sicurezza del loro portafoglio o tenendo le loro chiavi private o prendendo il controllo del software del portafoglio stesso. Noi usiamo un duplice approccio per attenuare questa minaccia.

PORTAFOGLI CALDI E FREDDI

Il primo approccio alla sicurezza dei portafogli è semplicemente non renderli disponibili agli attacchi online. È impossibile fare questo per tutti i portafogli per un cambiavalute o un sistema come Ducatus perché devono essere online per inviare monete ai membri. Ma ciò non significa che Ducatus ha bisogno di tenere tutte le sue monete online in ogni momento. Questo ha condotto al concetto portafogli caldi e portafogli freddi.

Ricordiamo che un portafoglio ha due componenti – le chiavi private e gli indirizzi pubblici. Le chiavi private sono richieste per elaborare il libro maestro delle transazioni, blockchain, per conto del portafoglio. Ogni portafoglio che ha un componete connesso a internet che conosce la sua chiave privata è chiamato portafoglio caldo per i nostri scopi. È vivo, online, e qualcosa che non vogliamo che sia raggiunto da qualcuno che lo attacchi. I portafogli usati da Ducatus per trasferire fondi ai membri devono essere caldi per inviare le transazioni al blockchain. I portafogli caldi Ducatus saranno fortemente garantiti durante le loro operazioni.

Un portafoglio freddo è un portafoglio che non è connesso a internet ma solo perché un portafoglio non è connesso alla rete delle monete Ducatus non significa che non riceva transazioni. I portafogli freddi sono tutti quelli che non hanno una connessione attiva, ma di cui noi conosciamo uno o più indirizzi pubblici. Le chiavi private potrebbero essere in una cassetta di sicurezza, ma gli indirizzi pubblici sono conosciuti dal libro mastro. Perciò, un portafoglio freddo può ricevere fondi sul blockchain anche se non è attivamente connesso.

La migliore pratica industriale la separazione del portafoglio – divide i fondi che sono disponibili per uno scambio tra un insieme di portafogli caldi e freddi. Questo significa che, anche se un portafoglio è attaccato con successo, la maggior parte dei fondi sono ancora intatti in tutti gli altri portafogli. Il distribuire oggetti su molti portafogli riduce il valore di ciascun portafoglio, rendendo l'attacco molto più difficile per ottenere degli oggetti di valore significativo. Le chiavi private del portafoglio freddo sono immagazzinate in un luogo fisicamente sicuro non accessibile su internet, e I portafogli caldi sono configurati per avere solo tante monete quante ci si aspetta siano necessarie su una base giornaliera. Mediante questo approccio assicuriamo che in ogni istante le minacce a cui siamo soggetti sono ridotte al minimo.

QUALITÀ DEL CODICE

La nostra sicurezza è buona solo quanto il nostro software, e il software usato per connettere il sito web Swissmine.club ai suoi portafogli caldi è un obiettivo principale per chi li vuole attaccare; I portafogli caldi sono dove chi esegue un attacco elettronico potrebbe accedere direttamente alle monete Ducatus. Noi ci siamo impegnati con esperti industriali in sicurezza delle informazioni per assicurare che il nostro processo e la nostra tecnologia siano incentrati sulla sicurezza, specialmente quando si tratta dei nostri portafogli caldi.

Noi usiamo una combinazione di controlli umani (sia ispezioni di terze parti sia l'uso di un gruppo di gestione interno quando vengono fatti significativi cambiamenti al codice sorgente) oltre a strumenti di analisi elettronica che possono aiutare a scoprire potenziali problemi tipo attacchi condotti immettendo nel codice comandi arbitrari attraverso applicazioni vulnerabili e possibili difetti logici. Questo non è qualcosa che facciamo una volta – la sicurezza è una preoccupazione continua ed è integrate nel nostro processo.

I PROSSIMI PASSI

A seguito dell'accettazione formale di questo libro bianco passeremo immediatamente alla fase esecutiva. Questo comporterà i seguenti passi:

1. Conferma delle specifiche riguardo il nuovo progetto software che parte dal codice Bitcoin esistente includendo l'identificazione di una specifica diramazione Bitcoin e stabilendo adeguati parametri.
2. Sviluppo del nuovo progetto software e uso efficace del nostro portafoglio Ducatus per il mining interno.
3. Fondazione del blockchain Ducatus seguito dall'inizio del mining anticipato delle monete Ducatus per Swissmine.club.
4. Selezione finale delle basi del codice per i componenti chiave (web / computer desktop / portafogli su dispositivi mobili, software di accesso alla base dati blockchain, eccetera)
5. Sviluppo e lancio del portafoglio web Ducatus e del software di accesso ai blocchi e integrazione con Swissmine.club.
6. Integrazione delle monete col negozio Ducatus.
7. Lancio dei portafogli su computer desktop e sui dispositivi mobili dei membri Ducatus.
8. Completamento degli strumenti per lo sviluppo del software applicativo per l'integrazione di Ducatus con i veditori web di terze parti e sistemi POS nei negozi.
9. Scambio interno delle monete Ducatus per il commercio tra membro e membro.
10. Completamento degli strumenti per lo sviluppo del software applicativo per sostenere gli scambi di criptovaluta con terze parti.

I prodotti finali chiave, in sequenza, saranno:

- Portafoglio Linux (usato per l'inizializzazione della blockchain)

- Mining anticipato delle monete Ducatus.
- Portafoglio basato sul web e software per la lettura dei blocchi; integrazione con Swissmine.club
- Portafogli Windows, OS X, Android, e iOS.
- Integrazione dei venditori di terze parti istruzioni/esempi/librerie.
- Mercato interno per gli scambi di monete Ducatus.
- Integrazioni degli strumenti per lo sviluppo del software applicativo di scambio di terze parti.

CONCLUSIONI

Ducatus è pronto a consegnare una soluzione robusta di criptovaluta per i membri della rete Swissmine.club. Abbiamo progettato un'architettura ben studiata basata sulle migliori pratiche industriali, il che significa che abbiamo davanti a noi un modo realistico per garantire una grande esperienza agli utenti. Durante lo sviluppo della nostra rete di monete ci siamo impegnati con esperti del settore delle blockchain e della sicurezza delle informazioni per assicurare la fornitura di una soluzione sicura e affidabile per nostri membri.