Guadagnare online con le criptovalute

GUIDA CRIPTOVALUTA

Pierluigi Tamanini

Guadagnare online con le cripto valute: Bitcoin e le Altcoin

(come guadagnare senza nessuna esperienza)

Sistema completo:

www.sistemarenditepassive.com

NB - prima di giudicare, inizia a leggere questo ebook**: dai una tregua al tuo *scetticismo* per due minuti!**

Introduzione

Il mio nome è Pierluigi Tamanini.

Sono uno scrittore, un ingegnere, un viaggiatore e – soprattutto – sono prossimo alla libertà finanziaria!

Ti ringrazio di essere qui e, se leggerai questo ebook fino in fondo, sono certo che sarai tu a ringraziarmi! :-)

Brevemente, voglio raccontarti la “mia storia”…

Cos’è una cripto valuta?

Citando Wikipedia:

“ Una **criptovaluta** (o crittovaluta o criptomoneta) è una valuta paritaria, decentralizzata digitale la cui implementazione si basa sui principi della crittografia per convalidare le transazioni e la generazione di moneta in sé. Come ogni valuta digitale, consente di effettuare pagamenti online in maniera sicura.

Le implementazioni di criptovalute spesso usano uno schema proof-of-work come salvaguardia alla contraffazione digitale. Esse utilizzano tecnologie di tipo peer-to-peer (p2p) su reti i cui nodi sono computer di utenti disseminati in tutto il globo. Su questi computer vengono eseguiti appositi programmi che svolgono funzioni di portamonete. Non c'è attualmente alcuna autorità centrale che le controlla. Le transazioni e il rilascio delle criptomonete avvengono collettivamente in rete, pertanto non c'è una gestione di tipo "centralizzato". Queste proprietà uniche nel suo genere, non possono essere esplicate dai sistemi di pagamento tradizionale.

Sono state definite oltre 30 diverse specifiche e protocolli di criptovalute per lo più simili o derivate dalla prima criptovaluta mai implementata, il Bitcoin. Ad oggi, tutte le criptovalute sono tutte valute alternative rispetto alle valute con valore legale.

La maggior parte delle criptovalute sono progettate per introdurre gradualmente nuove unità di valuta, ponendo un tetto massimo alla quantità di moneta che è in circolazione. Ciò viene fatto sia per imitare la scarsità (e il valore) dei metalli preziosi, sia per evitare l'iperinflazione. Comparata con le valute ordinarie gestite dagli istituti finanziari o tenute come contante, le criptovalute sono meno suscettibili a confische da parte delle forze dell'ordine. Le criptovalute esistenti sono tutte pseudonimi che consentirebbero l'anonimato.“

Forse avrai sentito parlare di gente che fatto i soldi coi bitcoin…

È tutto vero: il bitcoin è salito da 10 centesimi di dollaro a circa 20000$! (nel momento in cui leggerai questo scritto, magari varrà 1000000 di dollari!)

Quindi?

Quindi se anche tu vuoi guadagnare con le cripto valute, devi investire quando nascono, quando ancora

costano pochissimo.

Ecco perché il mio consiglio è di agire ORA, SUBITO, ADESSO!

Ora TI SPIEGO cosa intendo…

Non devi credermi per forza.

Fai bene ad essere scettico. Lo sono stato anch'io. È saggio essere scettico.

E ti dico una cosa: non investire mai denaro che non puoi permetterti di perdere! Mai!

Ma adesso stai per scoprire un paio di aziende che potranno

renderti davvero ricco…

Innanzitutto questa è la mia mail: Pierluigi.tamanini@gmail.com

Scrivimi e, se anche tu hai un account Gmail o Google, ti condividerò tutto il materiale che posseggo GRATUITAMENTE!

Sei ancora scettico, vero?
Bene, perfetto.
Allora dedica 20 minuti a guardare questo video sui bitcoin di SKY Tg24:

https://www.youtube.com/watch?v=rYhran_4R-A

Fatto?
Bene, se l'hai guardato, hai certamente capito che il futuro è BITCOIN, e non solo…

Ottimo.
Adesso proseguiamo.

Prima di presentarti la tua opportunità a lungo termine, vorrei presentarti un'opportunità un po' più rischiosa: Ethereum. Ma che dire di NEO? E di Dash!? Tron? Dentacoin? Ce ne sono circa 2000!!!

Scrivimi di renderò noto il mio crypto-portafoglio!
Non ora, segui il precorso

base e continua a leggere…

Ma prima di tutto, inizia a comprare i tuoi primi BITCOIN o BTC qui:

https://www.coinbase.com/join/5705d11

Sono sufficienti anche pochi EURO… se usi il link qui sopra riceverai 10 dollari in omaggio!

NB: FALLO ADESSO, SMETTI DI LEGGERE E ISCRIVITI!

Una volta comprato Bitcoin (più ne compri meglio è), sei già a metà dell'opera!

Adesso per diversificare potresti iniziare a comprare anche Litecoin LTC e Ethereum ETH

L'ideale sarebbe avere un portafoglio di questo tipo:

70% BTC

20% ETH

10% LTC

Prima di contattarmi vedi di trovarti nella situazione appena descritta!

Non avere fretta, inizia con 50€ e prosegui di settimana in settimana… poi passa a ETH e LTC.

Fatto? Sei pronto a proseguire?

CHE FARE ADESSO???

Adesso hai già le 3 migliori crypto in circolazione: bitcoin, ethereum e litecoin.

Proseguiamo?

Gli Exchange, ovvero dove comprare altre crypto e diversificare ulteriormente.

Innanzitutto installa sul tuo smartphone l'app GOOGLE AUTHENTICATOR. Ti tornerà utile.

Sai perché? La sicurezza è tutto in ambito crypto: ne parleremo più avanti.

Ora prenditi la briga di iscriverti a questi Exchange.

NB: non essere pigro, iscriviti a tutti! Altrimenti non potrai proseguire. Smetti di leggere e iscriviti adesso.

Usa questi link:

https://www.kucoin.com/#/?r=247Ht

https://www.binance.com/?ref=10209757

https://www.bitfinex.com/?refcode=ZT3Po2j0BH

https://www.cryptopia.co.nz/Register?

referrer=yonobusco

Adesso contattami pure via mail e discuteremo insieme sulle crypto del momento!

Non sono un advisor di crypto e non lo sarò mai, ma una bella chiacchierata via mail può aiutare entrambi!

Fatto? Proseguiamo parlando di sicurezza!

Argomento un po’ noioso ma molto importante!

Quelli che leggerai sono materiali che ho trovato in rete, mischiati l'uno con l'altro, un po' raffazzonati e aggiornati dal sottoscritto: fanne tesoro!

Ricordati che le cryptovalute possono farti guadagnare tanto, ma non segui le regole esposte qui sotto (almeno le principali) rischi di essere "rapinato" quando oramai eri convinto di essere ricco: occhio!

La regola è sempre la stessa: fai soldi e proteggili!

Prima di leggere tutto (o se non hai proprio voglia di leggere tutto): comprati il Ledger Nano, ovvero l'unico

modo sicuro per conservare il 90% delle crypto in circolazione:

https://www.ledgerwallet.com/r/f053

MANUALE DI SICUREZZA INFORMATICA PER CRIPTOVALUTE

Be you own bank, Be your own security

Ovvero sii la tua stessa banca!!!

Quando inizi a depositare fondi sulla blockchain, a cambiare valute e a spedire token da o verso un exchange fai delle operazioni senza nessun intermediario, dove sei tu stesso la tua banca. Questo comporta una responsabilità non solo per quanto riguarda le transazioni stesse ma anche in termini di sicurezza, in quanto il

terminale da cui operi, sia esso un laptop o uno smartphone, ci espone a potenziali rischi.

Ecco qui alcune regole e suggerimenti che ti aiuteranno a mantenere un buon livello di sicurezza durante le tue operazioni e la custodia dei tuoi fondi. Anche se alcune indicazioni ti sembreranno paranoiche è importante essere consapevoli di ogni rischio possibile

Tieni sempre aggiornato il tuo computer e il tuo smartphone

Installa sempre tutti gli aggiornamenti di sicurezza del sistema operativo, l'ultima versione dei browser Internet che usi e di tutte le applicazioni sul telefono. Un computer non aggiornato permette ad un hacker di sfruttare vulnerabilità conosciute. Non usare mai uno smartphone rooted per i tuoi wallet e le tue app dedicate alle criptovalute.

Dedica una lettura veloce agli articoli di sicurezza informatica per rimanere sempre aggiornato (e.g. Punto Informatico).

Per il tuo PC considera seriamente di passare a Linux, non esitare: c'è una comunità online disposta a supportare i principianti, e non devi fare il passaggio tutto in una volta in quanto puoi fare un sistema dual-boot o eseguibile da supporto USB. Ci sono OS come Qubes che garantiscono un alto livello di privacy e sicurezza, come Tails che funzionano perfettamente per sessioni live o come Linux Mint che è estremamente facile da usare anche per i principianti. Se usi MacOS o Windows assicurati di avere un malware detector e un firewall.

Assicurati che la tua connessione Internet sia sicura

Quando si va online in un luogo pubblico, ad esempio utilizzando una connessione Wi-Fi pubblica, non si ha alcun controllo diretto sulla sua sicurezza. Gli esperti di sicurezza informatica aziendale si preoccupano degli “endpoint”, i luoghi in cui una rete privata si collega al mondo esterno: il tuo endpoint vulnerabile è la tua connessione Internet locale. Assicurati che il tuo dispositivo sia sicuro e, in caso di dubbio, attendi un momento

migliore (ad esempio, fino a quando non sarai in grado di collegarti a una rete Wi-Fi sicura).

Disabilita il protocollo di sicurezza WPS se è abilitato sulla rete wireless; non usare mai lo standard WEP per la sicurezza wireless, utilizza solo il protocollo WPA2.

Considera seriamente un abbonamento un servizio di VPN

Il VPN aumenta notevolmente la sicurezza e la privacy durante l'utilizzo di internet, a casa ed è fondamentale averne uno quando si naviga in hotspot pubblici; evita i VPN gratuiti in quanto tengono i log di tutte le tue navigazioni, e quelli basati negli USA in quanto devono sottostare alle leggi americane dove l'intercettazione dei dati da parte delle autorità è una prassi.

VPN Consigliati: NordVPN o AirVPN

Backup

Fai un backup delle chiavi private (seed, file .json, Private Key) e NON salvarlo sul tuo computer: stampalo su un foglio o salvalo su un'unità esterna quali una chiavetta USB o una scheda SD. Procurati per questo scopo dei dispositivi nuovi che rispettino gli ultimi standard (e.g. USB 3.0) e siano affidabili perche non ti lascino a piedi. Se vivi con persone di cui non ti fidi completamente puoi proteggere ulteriormente i tuoi dati creando un folder criptato all'interno di questo supporto. Conserva questa carta o unità

esterna in più posizioni fisiche diverse (es. casa e ufficio). Un backup non è utile se viene distrutto da un incendio o da un'alluvione insieme al laptop. Non archiviare MAI la tua chiave privata su Dropbox, Google Drive o altro spazio di archiviazione nel cloud: se quell'account viene compromesso, i tuoi fondi verranno rubati.

Software di crittografia consigliati: LUKS o cryptsetup per Linux, VeraCrypt per Windows e FIleVault per MacOS.

Mantieni le impostazioni sulla privacy

Coloro che lavorano al marketing amano sapere tutto di te, e così fanno gli hacker. Entrambi possono imparare molto dalla tua navigazione e dall'uso dei social media. Hai però la possibilità di gestire quali tracce lasci online: sia i browser Web che i sistemi operativi mobili dispongono di impostazioni disponibili per proteggere la privacy online. I principali siti Web come Facebook hanno anche impostazioni di miglioramento della privacy disponibili. Queste impostazioni sono talvolta (volutamente) difficili da trovare perché le aziende vogliono le tue informazioni

personali per le loro attività di marketing. Assicurati di aver abilitato queste misure di protezione della privacy e di mantenerle abilitate. Considera l'utilizzo di motori di ricerca come DuckDuckGo che non tracciano le tue ricerche; copri la tua webcam con del nastro adesivo quando non la usi. Metti alla prova il grado di privacy del tuo browser su https://panopticlick.eff.org: sarai sorpreso nel vedere quante tracce stai lasciando nel web.

Last but not least: non lasciare MAI i tuoi address di Ethereum, Bitcoin o di qualsiasi blockchain in giro per nessun

forum, chat Telegram o Whatsapp, Facebook e in nessun luogo pubblico: con anche solo un indirizzo sarebbe facile risalire al tuo storico e quindi ai tuoi fondi. Per la stessa ragione non dire mai a nessuno quanto stai investendo o quanto sei disposto a investire, e come va la tua attivita finanziaria in genere.

Naviga solo su siti sicuri

Come non sceglieresti di attraversare a piedi un quartiere pericoloso, non

visitare i quartieri pericolosi online. I criminali informatici usano contenuti ambigui come esca. Sanno che a volte le persone sono tentate da contenuti dubbi e possono abbassare la guardia quando li cercano. Internet è pieno di insidie ▮▮ difficili da vedere, in cui un clic imprudente potrebbe esporre dati personali o infettare il tuo dispositivo con malware o con un ransomware. Resistendo all'impulso non dai nemmeno una possibilità agli hacker. Per la stessa ragione non andare MAI nel deepweb a meno che tu non sia pienamente consapevole di quello che stai facendo.

SCAM

Grazie anche alla crescente popolarità di Bitcoin e delle cripto valute in genere, gli SCAM su internet dedicati si stanno moltiplicando a dismisura. Se per i più navigati è facile riconoscere una truffa a colpo d'occhio per i nuovi del settore il rischio è più alto: non fidarsi mai di siti che propongono facili guadagni con slogan come double your bitcoin here. Ci sono decine di finti wallet (web e mobile) e pseudo servizi di investimento che non vi faranno mai

più rivedere i vostri sudati coin. Per la stessa ragione evita i gruppi di Pump, che sono fatti per arricchire solo i promotori del pump che vi venderanno i loro token quando cercherete di entrare, e naturalmente tutto ciò che ha l'aria di essere uno schema Ponzi. Fai riferimento a siti come www.badbitcoin.org anche solo nel più lieve dubbio.

Phishing

I siti dei wallet più popolari sono imitati alla perfezione per trarre in inganno l'utente che ignaro immette la propria chiave privata, ed ecco che i fondi spariscono in pochi minuti. Mettete nei segnalibri del browser gli exchange e i web wallet ai quali accedete per fare le operazioni e usateli sempre. Quando accedi ad un sito controlla sempre che l'indirizzo sia scritto correttamente e che sia presente il lucchetto verde:

Non fidarti di messaggi o link inviati a caso tramite email, Slack, Reddit, Twitter, ecc.

Passa sempre direttamente al sito tramite i tuoi bookmark prima di inserire le informazioni. Non inserire MAI informazioni dopo aver fatto clic su un collegamento da un messaggio o un'e-mail.

Installa un AdBlocker e non fare clic sugli annunci sul tuo motore di ricerca (ad es. Google).

Software consigliati: estensioni per browser uBlock, AdBlock, EtherAddressLookup

Scegli password sicure e attiva sempre il 2FA

Le password sono uno dei più grandi punti deboli dell'intera struttura di sicurezza di Internet, ma attualmente non c'è modo di aggirarli. E il problema con le password è che le persone tendono a scegliere quelle facili da ricordare (come "password" e "123456"), che sono anche facili da indovinare per i cyber-ladri. Seleziona password complesse che siano più difficili da capire per i criminali informatici. Una buona password è unica e complessa, lunga almeno 15 caratteri, che mescola lettere minuscole a maiuscole, numeri e caratteri speciali. Non scrivere mai le

tue password su un file testuale o di excel non criptato. Un software di gestione password può aiutarti a gestire più password in modo da non dimenticarle e da averle su tutti i dispositivi che usi: fai però attenzione alle estensioni di queste app nei browser (sono spesso prese di mira dagli hacker) e aggiungi sempre il 2nd Factor Authentication come ulteriore layer di sicurezza. Imposta il 2FA per tutti gli exchange ma anche per i social e le mail che usi normalmente: ogni fuga di dati potrebbe farti finire nel mirino di un hacker. Per questa stessa ragione potresti valutare di usare uno smartphone per il 2FA che non usi per accedere ai wallet o agli exchange.

Non usare gli SMS come 2FA in quanto il tuo numero di telefono potrebbe essere rubato da un hacker, o se vuoi usarlo imposta un numero apposito con la app Burner.

App / Software consigliati: per le password Keepass e LastPass, per il 2nd Factor Authentication Google Authenticator e Authy (backup automatico dei 2FA e anche app per Google Chrome)

Attento ai keylogger

I keylogger rappresentano una tipologia di spyware che registra tutto quello che viene immesso da tastiera, alcuni keylogger possono inoltre fare screenshot e accedere alla webcam; I keylogger possono anche essere hardware come ad esempio una chiavetta usb connessa nel retro del tuo pc. Se sospetti che il tuo PC sia infetto da un keylogger (a volte gli antivirus fanno fatica a individuarli), usa una tastiera virtuale e usa sempre il copia-incolla per le tue password (con un software di gestione delle password

questa operazione è molto più facile).

Usa una casella di email dedicata alle operazioni con le cripto valute

Non usare la stessa email che usi anche per i social o per il lavoro o per lo shopping, o servizi mail che hanno sofferto dei data breach. Per le criptovalute prediligi le mail con il massimo grado di sicurezza; impara a usare una chiave PGP per crittografare le tue mail e mantenere un alto grado di

sicurezza.

Servizi consigliati: Protonmail, Tutanota, Mailfence

Preferisci un hardware wallet come Ledger Nano S

Con un hardware wallet le tue chiavi private non usciranno mai dal dispositivo: l’unica maniera per rubare i tuoi fondi diventa la coercizione fisica (e purtroppo iniziano a esserci i primi

casi). Come recita il mini-corso sulla sicurezza di MyEtherWallet “ Se hai più di una settimana di valore in criptovaluta, prendi un portafoglio hardware. Niente scuse. Ne vale la pena. Te lo assicuro.”

Se non hai ancora il tuo Ledger Nano S utilizza solo i wallet consigliati da BCTop

I wallet consigliati soddisfano sempre due requisiti fondamentali:

Rendono possibile l’estrazione della Private Key, che ci permette di recuperare i fondi in ogni caso.

Non hanno vulnerabilità note

Inoltre sono i wallet su cui diamo pieno supporto.

Non lasciare mai i tuoi fondi sugli Exchange se non per il tempo indispensabile per fare le operazioni

Gli Exchange sono soggetti esterni fuori

dal nostro controllo: possono chiudere dalla mattina alla sera per qualsiasi motivo, possono venire derubati tramite un attacco informatico o possono semplicemente avere un problema interno per cui i tuoi fondi potrebbero venire congelati, e non si può fare molto affidamento sulla celerità del supporto.

Quando fai compravendita di cripto valute e hai bisogno di passare da un Exchange a un altro, fai sempre transitare i fondi dal tuo wallet

Se spediamo le valute direttamente da un Exchange a un altro rischiamo di vedere i nostri fondi intrappolati in uno Smart Contract e dobbiamo fare richiesta al supporto per sbloccarli: considerato il sovraccarico degli Exchange dovuto al boom di iscrizioni (è il rovescio della medaglia della popolarità delle cripto valute) è meglio non avere frequente bisogno del supporto. Prioritizza le transazioni dal tuo wallet (purtroppo non puoi farlo da Exchange) ad esempio aumentando il GAS e i GWEI se sei sulla blockchain di Ethereum per fare i tuoi trade più velocemente.

Controlla sempre almeno 2 volte l’address a cui stai mandando i tuoi fondi e usa sempre la funzione copia-incolla per scrivere gli indirizzi.

Un indirizzo con una lettera sbagliata significa mandare i nostri fondi a un wallet di cui non abbiamo controllo, quindi equivale alla totale ed irrimediabile perdita dei fondi. Anche facendo copia incolla si corrono però dei rischi, ci sono infatti dei malware in circolazione che quando riconoscono un indirizzo Bitcoin nella clipboard (e presto arriveranno anche le altre valute)

lo cambiano con l'indirizzo dell'hacker: quindi è buona prassi controllare più volte che l'indirizzo originale e quello copiato siano identici.

Per partecipare a un ICO usa solo wallet di cui possiedi le chiavi private e MAI da un exchange

Non partecipare MAI spedendo fondi da un exchange o da un wallet non consigliato da BCTop in quanto potresti non ricevere mai i tuoi token. Se

partecipi alla ICO da smartphone, prediligi il wallet Eidoo che grazie al suo ICO Engine non richiede l'indirizzo a cui donare oppure, nel caso la ICO non sia supportata da Eidoo, verifica più volte l'address a cui stai mandando i tuoi soldi controllando più fonti e contattando direttamente il supporto ufficiale della ICO. Controlla sempre i canali Medium, Slack e Twitter ufficiali della ICO per rimanere aggiornato su eventuali falle di sicurezza emerse durante la campagna di raccolta fondi.

FINE

ALLORA???

CHE NE PENSI???

Ok, probabilmente non ci hai capito niente, o quasi.

Bene, allora fai la cosa giusta e più semplice…

Dopo aver letto tutto (o se non hai proprio voglia di leggere tutto): comprati il Ledger Nano, ovvero l'unico modo sicuro per conservare il 90% delle crypto in circolazione:

https://www.ledgerwallet.com/r/f053

Un saluto e… ci sentiamo presto!

Pierluigi

www.sistemarenditepassive.com