Il Codice Pirata

V1.0

Di: Flexatron, FishyGuts, jl777c e Comunità KMD

Sintesi

Una criptovaluta completamente privata e una blockchain schermata originati dall'ecosistema di Komodo. Pirate risolve il "problema di fungibilità" di Zcash attraverso l'eliminazione della funzionalità di transazione verso indirizzi in chiaro nella sua blockchain, rendendo l'uso privato "infallibile". Questa caratteristica si traduce in una base di monete utente completamente schermata nella catena di Pirate. Usando costantemente la tecnologia zk-SNARK, la moneta pirata non lascia metadati utilizzabili delle transazioni dell'utente sulla sua blockchain. Tutto le transazioni in uscita, diverse dai premi sui blocchi del mining e le transazioni notarili, vengono inviate agli indirizzi *Sapling* schermati massimizzando l'efficienza e velocità della sua catena. Pirate utilizza l'algoritmo di consenso Equihash, verifica di computo creata da Zcash, con un ulteriore livello di sicurezza di verifica posticipata di computo o dPoW, data da Komodo che fornisce un valore superiore come sicurezza a quello del BTC per la blockchain Pirate. Il futuro dei pagamenti decentralizzati privati è qui.

Indice

Il Codice Pirata

Lo statuto della Missione

La missione di Pirate è di preservare la privacy finanziaria delle persone in un sistema dominato da transazioni in chiaro.

Proposte di valore

Tutte le transazioni sulla catena Pirate sono private per impostazione predefinita.

Questo allevia i problemi di fungibilità che molte criptovalute con privacy opzionale introducono nel loro protocollo. Questo protocollo completo sulla privacy offre agli utenti una maggiore garanzia che nessuna autorità è in grado di affermare che i fondi degli utenti sono "macchiati" a causa di transazioni precedenti, ora e in futuro.

Pirate Coin è completamente decentrata.

Non ci sono terze parti responsabili dei tuoi fondi in qualsiasi momento. Le transazioni private sono confermate in modo fidato sulla blockchain, il che significa che non hai bisogno di una terza parte per verificare che le tue transazioni siano valide, il codice pirata si prende cura di questo.

Pirate consente un trasferimento sicuro e rapido del valore.

La catena dei pirati è protetta da un meccanismo più difficile da decifrare rispetto al bitcoin, chiamato prova di lavoro ritardata (dPoW). Le tariffe di utilizzo sono molto economiche sia per il cliente che per il venditore. Inoltre, non vi è alcuna possibilità di rimborso fraudolento, nessun periodo di verifica fondi errati e le transazioni sono confermate e protette in pochi minuti. Solo queste caratteristiche possono far risparmiare ai commercianti e venditori in tutto il mondo miliardi di dollari riducendo le commissioni di agevolazione.

Pirate utilizza il protocollo di privacy più resistente.

Il protocollo sulla privacy altamente avanzato e rispettato, zk-SNARKS, non richiede che i dati della transazione siano visibili sui libri contabili pubblici. Questo è considerato da molti importanti sviluppatori come uno dei metodi più efficaci per nascondere i dati finanziari sulla blockchain

Perché concentrarsi sulla privacy?

Il mondo Cripto offre vantaggi agli utenti e alle aziende, ma ciò non dovrebbe avvenire a scapito della privacy finanziaria.

Le valute FIAT odierne stanno già facendo un esodo di massa verso i sistemi digitali (Japparova en Rupeika-Apoga 2017). Le Criptovalute hanno dimostrato di offrire numerosi vantaggi per le aziende, come ad esempio il risparmio sui costi delle tasse e la velocità delle transazioni. A nostro avviso, gli utenti meritano la privacy in tali transazioni.

Perché mostrare al proprietario del negozio le dimensioni della tua ricchezza o le tue abitudini di spesa?
La privacy finanziaria può quindi essere necessaria per tutte le parti che desiderano accettare criptovaluta come venditori, distributori, commercianti, acquirenti, fornitori, fornitori di servizi e clienti. Le aziende possono assicurare i propri clienti e sé stessi che entrambe le parti della transazione riceveranno la migliore combinazione di privacy, velocità e risparmi sui costi grazie all'utilizzo di Pirate.

Il team
Essendo una criptovaluta veramente decentralizzata, Pirate, dà il benvenuto agli sviluppatori e ai contributori con ogni tipo di abilità e capacità.

Già oltre 30 contributori hanno fornito servizi per la crescita e lo sviluppo della catena dei pirati sin dalla sua infanzia. Gli sviluppatori stanno lavorando in modo coerente in team per portare conoscenza ed esperienza da tutte le parti della cripto-sfera. Con il nostro gruppo eterogeneo, c'è sempre una persona con la conoscenza di come completare un compito necessario, o qualcuno con una connessione a qualcuno che può farlo.

Pirate ha raggiunto molti traguardi per prima nel settore delle criptovalute quando si tratta di protezione della privacy (vedi Tabella di marcia) e Pirate continuerà a collaborare con terze parti su tecniche innovative per facilitare la privacy per tutti.

Criptovalute

Dalla pubblicazione del famoso libro bianco scritto da Satoshi Nakamoto nel 2008 (Nakamoto 2008), Bitcoin è diventato un bene digitale con capitalizzazione di mercato da molti miliardi di dollari. Un certo numero di criptovalute alternative hanno generato da allora il tentativo di riempire il vuoto di una pletora di casi d'uso, con le loro rispettive comunità. L'uso delle criptovalute come mezzo di pagamento è uno dei casi d'uso più popolari e anche lo scopo principale per cui Satoshi ha scritto il white paper. L'obiettivo di Bitcoin è quello di consentire ad ogni persona di trasferire valore in qualsiasi parte del mondo in qualsiasi momento, utilizzando istantaneamente una connessione Internet in modalità peer-to-peer, senza doversi affidare a nessuna terza parte. Bitcoin utilizza un libro mastro distribuito per facilitare e registrare transazioni di cui la veridicità è determinata tramite l'algoritmo di consenso Proof-of-Work (PoW).

Privacy

Una grande preoccupazione per l'utilizzo di questa tecnologia è la capacità degli osservatori di analizzare il comportamento di spesa e lo stato di ricchezza (Moser 2013). Ciò compromette enormemente la privacy finanziaria dell'utente. Sono stati sviluppati numerosi protocolli di criptovaluta che cercano di migliorare gli aspetti della privacy di Bitcoin. I protocolli più importanti che sono stati sviluppati fino ad ora sono CryptoNote (Van Saberhagen 2013) e Zerocash (Sasson et al., 2014). Il primo protocollo utilizza Ring Confidential Signatures, mentre il secondo utilizza prove a conoscenza zero per offuscare le transazioni e i saldi dei conti, più in dettaglio su quello successivo. Entrambi i protocolli hanno i loro vantaggi e svantaggi. Questo whitepaper affronta il modo in cui Pirate (ARRR) tenta di migliorare gli aspetti relativi alla privacy degli attuali protocolli di pagamento decentralizzati.

Principali inconvenienti illustrati degli attuali protocolli di pagamento decentrati

Schema delle firme Ring CT di Monero

Monero, un fork di Bytecoin basato sul protocollo CryptoNote, utilizza uno schema di firme ad Anello nelle loro transazioni, combinato con indirizzi nascosti, indirizzi casuali monouso per ogni transazione per conto del destinatario. Le firme ad Anello rendono sempre più difficile rintracciare il mittente in base alla dimensione dell'anello. Tuttavia, questo lascia alla capacità di

terze parti di analizzare i dati disponibili con sofisticati strumenti analitici in questo momento e in futuro.

A causa del suo uso delle firme ad anello, l'analisi della blockchain di Monero è difficile, come mostrato nella Figura 1.

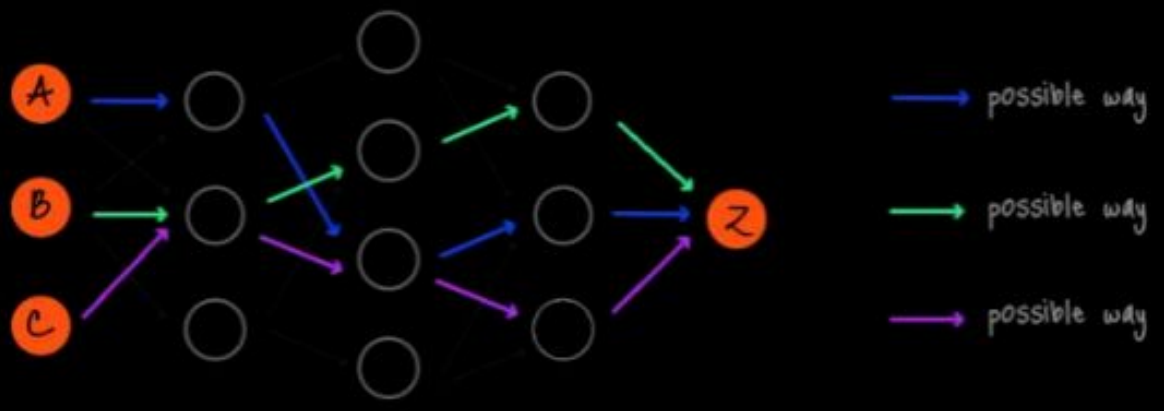

Figura 1 Analisi della blockchain della firma ad anello. Fonte: https://cryptonote.org/inside#untraceable-payments

La difficoltà nel trovare il mittente corretto è sempre più difficile con gli anelli di dimensioni maggiori. La dimensione dell'anello è il numero totale di possibili firmatari compreso il tuo, che a sua volta determina la complessità e la difficoltà di trovare il "risultato reale". Maggiori dimensioni dell'anello forniscono quindi un livello di privacy più elevato rispetto a quelle inferiori. Tuttavia, non è consigliabile riutilizzare un numero dispari di dimensioni dell'anello riconoscibile per evitare di distinguersi da altre transazioni [3]. Il problema fondamentale dei metodi di mescolamento delle monete è che i dati delle transazioni non vengono nascosti tramite la crittografia. RingCT è un sistema di dissociazione in cui l'informazione è ancora visibile nella blockchain. Ricorda che in futuro potrebbe essere scoperta una vulnerabilità che consente la tracciabilità poiché la blockchain di Monero fornisce un record di ogni transazione che ha avuto luogo.

Implementazione di indirizzi schermati Zcash e tipi di spesa

Zcash, un'implementazione del sistema di pagamento anonimo decentralizzato Zerocash, aggiunge uno schema di pagamento protetto da argomenti di conoscenza succinti non interattivi non informativi(zk-SNARKs) allo schema di pagamento trasparente esistente utilizzato da Bitcoin (Hopwood et al.2016). L'utente può scegliere se usare pagamenti protetti o no. Si presume che la percentuale di transazioni protette aumenterà vista la recente implementazione di "Sapling" in Zcash che rende l'elaborazione di transazioni schermate solo una frazione più intensiva dal punto di vista computazionale delle transazioni non protette (Bowe 2017). Sfortunatamente, la percentuale relativamente elevata di transazioni e conti non schermati altera la fungibilità delle monete, in quanto è possibile collegare transazioni durante l'attività di pagamento "private" e quindi eventualmente relazionarle al mixaggio di monete. Questo è specialmente il caso della conduzione di una "transazione di andata e ritorno", che significa inviare un numero esatto di monete da un indirizzo trasparente non schermato (t-addr) a un indirizzo schermato (z-addr) e indietro ad un altro indirizzo non protetto (Quesnelle 2017). Ci riferiamo a questo documento su questo fenomeno come "problema di fungibilità".

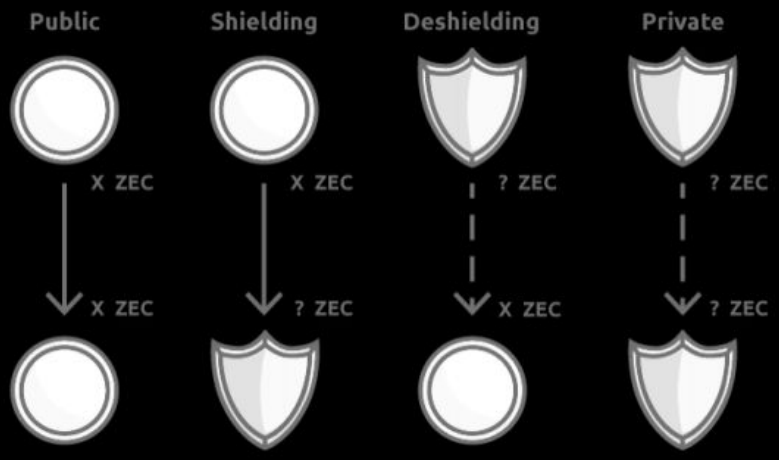

Figura 2 Gli utenti di Zcash hanno 4 diverse opzioni di spesa Zcash. Fonte: https://z.cash/blog/sapling-transaction-anatomy/

Come visto in Figura 2, gli utenti Zcash hanno la possibilità di condurre 4 diversi tipi di transazioni col protocollo Zcash corrente. Essere in grado di inviare da un indirizzo pubblico ad uno protetto e viceversa mette a repentaglio la fungibilità delle monete. È possibile identificare i modelli di miscelazione delle monete tra i diversi tipi di transazioni quando gli utenti inviano

monete a indirizzi trasparenti, come nel caso delle "transazioni di andata e ritorno", poiché questo comportamento ha dimostrato di avere un'elevata connettibilità (Quesnelle 2017) .

Gli aggiornamenti delle prestazioni di Sapling, purtroppo, hanno un costo in privacy, in quanto le transazioni di Sapling rivelano più metadati rispetto alle "vecchie" operazioni tradizionali di JoinSplit. Le transazioni di sapling mostrano il numero di input e output utilizzati. Questa funzionalità aumenta le opzioni per differenziare i tipi di transazione, analizzare i dati delle transazioni ed eventualmente identificare il comportamento correlato al missaggio. Per ridurre o eliminare questo rischio è importante ridurre l'utilizzo di indirizzi trasparenti o semplicemente disabilitarlo dall'inizio in una nuova blockchain come Pirate.

La nostra soluzione

Pirate mira a migliorare in modo sostanziale rispetto alle caratteristiche di privacy e sicurezza di Monero e a risolvere il "problema di fungibilità" di Zcash. La catena dei pirati lo fa accettando soltanto transazioni schermate "Sapling" (z-tx), a parte i guadagni del mining e le autenticazioni notarili, come spiegato nella sezione dPoW. Inoltre, la catena dei pirati è protetta attraverso il meccanismo verifica posticipata del computo che rende la sua privacy e le caratteristiche di sicurezza attualmente ineguagliate nel settore delle blockchain rispetto alle monete della privacy esistenti.

La catena PIRATE: privacy, fungibilità e sicurezza

29 agosto 2018 - Il bisogno per il vero anonimato

Pirate è nata il 29 agosto in Discord come idea di una moneta al 100% zk-SNARKS. Il lavoro di sviluppo di *jl777c* sulle blockchain create indipendenti da Komodo o catena parallela, ha permesso di rafforzare l'utilizzo delle transazioni protette adeguando i parametri di attività delle catene parallele in una nuova catena parallela (Grewal2018). Una catena parallela è un fork del runtime di Komodo ed è una vera e propria blockchain indipendente. Inizialmente Pirate è iniziato come un esperimento per osservare se le z-transazioni forzate avrebbero funzionato, ma la comunità ha realizzato rapidamente il suo potenziale dopo che *jl777c* ha implementato con successo la verifica di computo posticipata rendendo Pirate essenzialmente completo.

Komodo - Fork di Zcash - zk-SNARKs

Pirate è una catena parallela parte dell'ecosistema della piattaforma Komodo. Il progetto Komodo si concentra sul potenziamento degli imprenditori blockchain e degli utenti di criptovaluta media con libertà e facilità d'uso attraverso la tecnologia blockchain (Lee 2018). Komodo è iniziato come un fork della famosa moneta per la privacy, Zcash. Il progetto Zcash è di per sé un fork di Bitcoin. Quindi, tutte le funzionalità progettate da Satoshi Nakamoto nel protocollo Bitcoin sono disponibili anche in Komodo. In quanto tale, Komodo conserva le stesse caratteristiche di privacy di Zcash.Tra queste funzionalità ci sono i parametri Zcash e la tecnologia zk-SNARK. Zk-SNARKS è una delle forme più potenti di privacy su blockchain esistente, in quanto la privacy fornita è effettivamente permanente.

Questa affermazione è anche evidenziata dal rappresentante principale di Monero, *Riccardo "fluffypony" Spagni*:

"zkSNARKs di Zcash offre caratteristiche di non tracciabilità molto più forti di Monero (ma un set di privacy molto più piccolo e rischi sistemici molto più elevati)."

catena parallela di Komodo

Una catena parallela (ufficialmente Catena Parallela) è una blockchain creata in modo indipendente che eredita tutte le

funzionalità di Komodo come la compatibilità di BarterDEX, la Privacy Zero-Knowledge e la verifica posticipata di computo ecc. ma ha anche numerose specifiche personalizzate, come fornitura di monete personalizzate e porta RPC personalizzata. Altre funzionalità personalizzate sono attualmente in cantiere per essere aggiunte (PTY X 2018).

Altri esempi di catene parallele di Komodo includono Bitcoin Hush (BTCH), ChainZilla (ZILLA), DEX, Equalizer (EQL), KMDice, Monaize (MNZ), PUNGO, REVS, SuperNET, Utrum e ZEX.

Z-transazioni Obbligatorie

La migliore soluzione al "problema di fungibilità" è di disabilitare la possibilità di inviare a indirizzi non protetti, a nostro avviso. Ciò elimina l'esistenza di transazioni da conti protetti a conti trasparenti che sono spesso la causa principale della diminuita fungibilità. Come citato dal principale sviluppatore Zcash in risposta al documento intitolato "Sulla connettibilità delle transazioni Zcash" di Jeffrey Quesnelle:

"Ma la mia risposta è invece che vieteremo le transazioni non protette. Ancora più semplice."

Verifica Computazionale Posticipata: massima sicurezza e flessibilità

Che cosa è la Verifica Computazionale Posticipata?

La Verifica Computazionale Posticipata deriva da Komodo e fornisce una forma di sicurezza unica e innovativa che è forte quanto la rete alla quale si collega ma non richiede i costi per eseguire quella rete. La Verifica Computazionale Posticipata è una soluzione che utilizza più metodi esistenti in un unico sistema di consenso ibrido che è efficiente dal punto di vista energetico come la Verifica di Impegno o Proof of Stake (PoS) pur essendo protetto dalla Verifica Computazionale di Bitcoin. Gli utenti che creano blockchain indipendenti (catena parallela) nell'ecosistema di Komodo possono scegliere di avere un hash di blocco, che serve da "istantanea" della propria blockchain inserita nella catena principale di Komodo. In questo modo, i dati della catena parallela sono inclusi indirettamente nel blocco-hash di Komodo che viene inserito nella blockchain della rete più forte (ora Bitcoin). Quindi dPoW consente anche alle più deboli blockchain di trarre beneficio dal tasso computazionale di Bitcoin e questo, a sua volta, rende l'utilizzo di energia di Bitcoin più ecologico e protegge l'intero ecosistema di dPoW oltre che sé stesso (Jl777c 2016). Oltre a Pirate, dPoW è stato implementato con successo in un gran numero di catena parallela come Game Credits, Einsteinium (EMC2), Pungo e HUSH, tra gli altri (Komodostats 2018).

Quali sono i meccanismi alla base della Verifica Computazionale Posticipata?

Il servizio di sicurezza Komodo viene eseguito da nodi notarili che sono necessari per registrare hash dei blocchi sulla blockchain di Bitcoin, noto come autenticazione notarile (Figura 3). L'autenticazione notarile comporta la creazione di una transazione bitcoin firmata di gruppo contenente il block-hash più recente di Komodo, firmato da una combinazione sconosciuta di 33 dei 64 nodi notarili (Jl777c 2016). Gli hash dei blocchi della catena di Pirate (tra le altre catene parallele) sono inseriti nella blockchain di Komodo in modo tempestivo e utilizzano lo stesso metodo. In questo modo, anche una singola copia sopravvissuta della catena principale di Komodo consentirà a tutto l'ecosistema di catene di risorse di sovrascrivere e annullare qualsiasi tentativo di modifica da parte di un aggressore. I nodi notarili pagano la commissione di transazione Bitcoin per autenticare la blockchain di Komodo. I costi delle commissioni di transazione bitcoin per i nodi notarili sono compensati dai premi di blocco e dalle commissioni delle transazioni della blockchain di Komodo inviate ai nodi notarili. Si prevede pertanto che gli interessi finanziari delle parti interessate vadano a votare per i nodi notarili con cui le parti interessate sono a proprio agio. 64 nodi notarili ampiamente distribuiti sono in attesa di elezione e dovrebbero essere una rappresentazione ottimale di un ecosistema decentralizzato che rende altamente improbabile qualunque tipo di attacco del 51%.

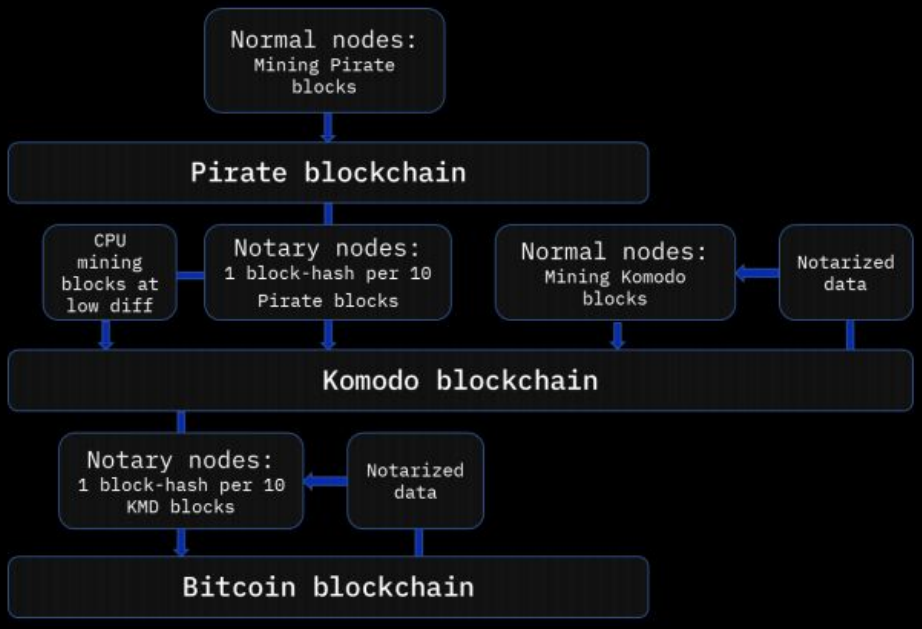

Figure 3 Una rappresentazione schematica della Verifica Computazionale Posticipata.

Quindi, per riorganizzare e attaccare Pirate, l'attaccante dovrebbe distruggere:

- tutte le copie esistenti della catena dei Pirati;
- tutte le copie della catena principale di Komodo;
- la rete di sicurezza PoW (Bitcoin) in cui sono inseriti i dati notarili della blockchain di Komodo.

Inoltre, i nodi notarili hanno la libertà di passare il processo di autenticazione notarile a un'altra rete PoW se in futuro si verifica uno spostamento dei tassi di hash tra le grandi blockchain. La verifica computazionale posticipata fornisce a Pirate una sicurezza superiore a quella di Bitcoin, evitando allo stesso tempo costi finanziari eccessivi ed eco-ostili. Grazie alla flessibilità di dPoW offre una natura più flessibile e adattabile rispetto al Bitcoin stesso.

Esempi di attacchi alle blockchain

Vi sono numerosi esempi che evidenziano la necessità di un meccanismo come la verifica computazionale posticipata: nell'aprile 2018, un bug nel meccanismo di retargeting degli algoritmi di Verge (XVG) è stato sfruttato per mezzo di un Attacco del 51%. Usando i timestamp falsificati, la necessità di un algoritmo diverso è stata elusa ad ogni blocco. Gli hacker sono stati in grado di inviare blocchi alla catena a una velocità di 1 blocco al secondo, negando di fatto il 99% dei blocchi dei legittimi pool e facendogli perdere denaro (Ocminer 2018a). Nel maggio 2018 si è verificato lo stesso attacco ma con un approccio diverso: gli hacker hanno inviato un blocco con l'algoritmo Scrypt contenente un timestamp falsificato seguito da un blocco con l'algoritmo Lyra2re contenente un timestamp falsificato e ripetendo tale processo e riducendo così la difficoltà, gli hacker erano in grado per estrarre diversi blocchi al minuto (Ocminer 2018b). Il 16 maggio 2018, Bitcoin Gold è stato attaccato da uno sconosciuto che è riuscito a rubare oltre 388.000 BTG dagli scambi di criptovalute, durante l'attacco le monete valevano 17,5 milioni di dollari (Roberts 2018). NiceHash offre attualmente più di una sufficiente potenza di hash in affitto per attaccare un numero di criptovalute di piccole e medie dimensioni. Il termine "Nicehashable" è stato coniato per la possibilità di noleggiare hash per attaccare una moneta e i siti sono già spuntati per mostrare le opportunità di hacking (EXAKING 2018).

Integrazione e attivazione del Sapling

Integrazione del Sapling

L'integrazione di Sapling nella catena di Pirate è stata un successo grazie alla cooperazione tra i membri dell'ecosistema Komodo, con un ringraziamento speciale a Mike Toutonghi del progetto Veruscoin. Pirate è sinonimo di transazioni rapide, economiche e al 100% private e Sapling è la migliore versione della tecnologia zk-SNARKS che le offre. Per questo motivo, l'utilizzo di Sapling è forzato dal 15 febbraio 2019 in poi per assicurarsi che la catena funzioni in modo efficiente e privato. Gli utenti che possiedono Pirate devono migrare le loro monete dai loro indirizzi Sprout agli indirizzi Sapling prima di quella data. La tempistica dell'attivazione dell'hard-fork per Sapling era basata su un timestamp a blocchi intorno al 15 dicembre, 1 ora UTC. La scadenza per la migrazione da Sprout a Sapling è stata fissata al 15 febbraio 2019 per creare un senso di urgenza e coinvolgere tutti i pirati. Prima viene eseguita la migrazione, migliore è la situazione degli scambi centralizzati e di altre app di terze parti. Un'app decentralizzata (dApp) chiamata "zMigrate" che converte automaticamente i fondi dell'utente in indirizzi di Sprout in un indirizzo Sapling è stata sviluppata da *jl777c* per semplificare il processo di migrazione a Sapling. Tutti i nodi dovevano necessariamente completare questo processo entro il 15 febbraio 2019 e anche le pool hanno fatto il salto verso gli indirizzi di Sapling dopo l'hard-fork.

La migrazione a Sapling

La dApp zMigrate è un programma che interagisce con il software "Komodod". La dApp invierà i Pirate negli indirizzi Sprout dell'utente a un indirizzo trasparente randomizzato utilizzato una sola volta per un massimo di 10.000 pirati per transazione. Siccome vengono creati tanti indirizzi t usa e getta quanti sono necessari per spostare tutti i fondi, con l'ultima transazione probabilmente conterrà meno di 10 K (a meno che i fondi non siano divisibili per 10 K). Di conseguenza, i fondi provenienti da ciascun indirizzo t vengono inviati all'indirizzo Sapling protetto designato. In questo modo l'utente ha il controllo dei fondi per tutto il tempo e il movimento di fondi trasparenti sarà il più omogeneo possibile per ridurre il danno alla fungibilità della catena. Il risultato del processo è che tutti i fondi dell'utente vengono trasferiti dal vecchio indirizzo Sprout al loro indirizzo di scelta Sapling.

I miglioramenti tecnici di Sapling consentono lo sviluppo delle seguenti funzionalità:

- Integrazione Punto vendita e Portafogli hardware
- Web Shop Plug-in (in arrivo)
- Portafogli mobili attraverso l'attivazione di Simple Payment Verification (Verifica di Pagamento Semplice) (zSPV) (in fase di sviluppo)

Schema delle emissioni e caratteristiche tecniche

La catena Pirate contiene le seguenti caratteristiche tecniche e non dopo il 15 dicembre:

- Algoritmo di estrazione: prova di computo Equihash
- Verifica Computazionale Posticipata
- Tempo per blocco: 60 secondi
- Commissione di transazione: 0,0001 ARRR
- Registrazione delle transazioni in pochi secondi
- Transazioni al secondo: 50-80 TPS
- Invia fondi fino a 100 indirizzi in un'unica transazione
- Dimensioni Tx di + o - 2000 byte con un massimo di 200 kB
- Utilizzo della memoria di soli 40 MB (Raspberry Pi)
- Dimensione del blocco di 4 mB massimo
- Visualizzazione di chiavi che offrono la possibilità di mostrare tutte le transazioni inviate da un indirizzo assegnato
- Capacità di generare un numero "infinito" di portafogli "Lite"

PROGRAMMA DI EMISSIONE

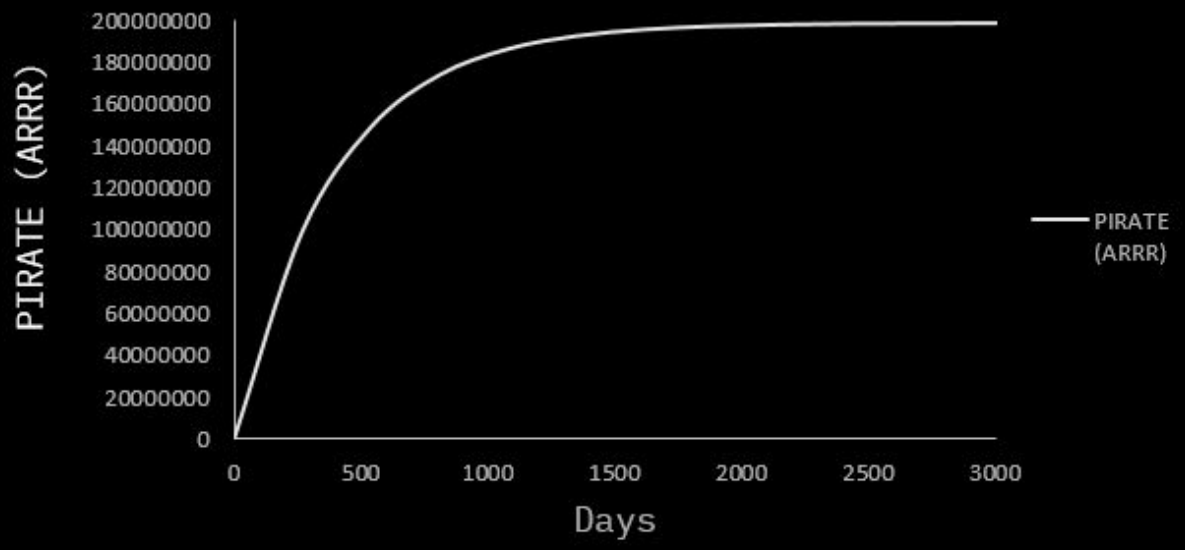

Figura 4 Il programma di emissione di Pirate (ARRR)

C'è un evento di dimezzamento dei premi per blocco ogni 388885 blocchi che equivale a circa 270 giorni. La fornitura totale è stimata a circa 200 milioni di Pirate (ARRR).

Supporto TOR

È possibile eseguire la catena Pirate sulla rete TOR e offuscare il proprio indirizzo IP, un numero collegato alla propria posizione geografica. Come utente hai bisogno di un browser TOR e delle binarie di Komodo per essere in grado di eseguire la catena di Pirate. Una guida passo-passo è disponibile sul sito pirate.black. La richiesta di supporto TOR è stata condivisa con gli sviluppatori di Agama Wallet. Una volta fatto, impostare Tor per una moneta o una catena parallela è molto semplice.

Supporto degli scambi centralizzati

La comunità non era sicura se gli scambi centralizzati sarebbero stati in grado di accettare Pirate in un primo momento a causa della mancanza di indirizzi trasparenti. Non molto tempo dopo la nascita di Pirate, Pirate ha lavorato con sviluppatori di un'exchange e programmatori per facilitare l'uso di depositi e prelievi su indirizzi Z per primi al mondo. Questo particolare scambio è DigitalPrice e ha lanciato con successo il trading a fine ottobre 2018.

Le date delle seguenti caratteristiche e sviluppi di terze parti (come Tortuga) sono stime basate su una base trimestrale e listate in ordine di aspettativa.

Tabella di marcia

Le seguenti caratteristiche da sviluppare di PIRATE sono stime basate su un periodo trimestrale in ordine di aspettativa.

Pool con pagamenti al 100% su indirizzi Z	Q3 2018 (completato)
Primo bot per mance su indirizzi Z su discord	Q3 2018 (completato)
Facilitare indirizzi Z su un CEX	Q3 2018 (completato)
Portafogli di carta	Q4 2018
Rifacimento Sito web	Q4 2018
Sistema referral	Q4 2018
Bot Lotteria Pirate	Q4 2018
Sapling	Q1 2019
Fondazione Pirata	Q1 2019
Tortuga (CEX)	Q1 2019
Verifica Semplice Pagamento (zSPV)	Q2 2019
Integrazione portafogli hardware	Q3 2019

La Guida a PIRATE

Imbarco su Pirate

Compra facilmente e in sicurezza piccole quantità di ARRR:
https://dexstats.info/onboarding.php

Come minare

Calcola i tuoi guadagni con una stima:
https://dexstats.info/piratecalc.php
Iniziare:
https://medium.com/piratechain/how-to-mine-pirate-step-by-step-withgpu-s-4c98f3dbcf5e
Scegli una pool qui:
https://miningpoolstats.stream/pirate
Tieni d'occhio l'hashrate di PIRATE:
https://dexstats.info/piratehash.php

Compra e scambia PIRATE

Registrati su DigitalPrice e negozia ARRR contro BTC, ETH o KMD:
https://digitalprice.io/?inviter=4fdaf7 (ref. link ufficiale PIRATE)

Social media

Pirate è attivo su Bitcointalk, Discord, Medium, Reddit, SteemIt, Telegram, Twitter e listato sul sito statistico per criptovalute CoinPaprika.
https://coinpaprika.com/coin/arrr-pirate/
https://discord.gg/mBZhZgz
https://medium.com/@piratechain
https://www.reddit.com/user/piratechain
https://steemit.com/@piratechain
https://twitter.com/PirateChain
https://t.me/piratechain
https://bitcointalk.org/index.php?topic=4979549.0

Codice sorgente e portafogli

Github: https://github.com/PirateNetwork
Portafogli Agama: https://github.com/KomodoPlatform/Agama/releases
Portafogli GUI PIRATE: https://github.com/leto/TreasureChest

Riferimenti

Bowe, S. 2017. “Cultivating Sapling: Faster zk-SNARKs--Zcash Blog”. Zcash Blog.

EXAKING. 2018. “PoW 51% Attack Cost”. 2018. https://www.exaking.com/51.

Grewal, Satinder. 2018. “Satinder’s notes on the PIRATE chain”. 2018. https://blog.komodoplatform.com/pirates-of-komodo-platform-cdc991b424df.

Hopwood, Daira, Sean Bowe, Taylor Hornby, en Nathan Wilcox. 2016. “Zcash protocol specification”.

Japparova, Irina, en Ramona Rupeika-Apoga. 2017. “Banking Business Models of the Digital Future: The Case of Latvia”. European Research Studies 20 (3A). Professor El Thalassinos: 846.

Jl777c. 2016. “Delayed Proof of Work (dPoW) Whitepaper”. Github. 2016. https://github.com/KomodoPlatform/komodo/wiki/Delayed-Proof-of-Work-(dPoW)-Whitepaper.

Kappos, George, Haaroon Yousaf, Mary Maller, en Sarah Meiklejohn. 2018. “An Empirical Analysis of Anonymity in Zcash”. arXiv preprint arXiv:1805.03180.

Komodostats. 2018. “Asset Chains Notarizations Summary”. 2018. https://komodostats.com/acs.php.

Lee, James. 2018. “Komodo: An Advanced Blockchain Technology, Focused on Freedom.” Komodo. 2018.

Moser, Malte. 2013. “Anonymity of bitcoin transactions”.

Nakamoto, Satoshi. 2008. “Bitcoin: A peer-to-peer electronic cash system”. Working Paper.

Ocminer. 2018a. “Network Attack on XVG / VERGE”. Bitcointalk. 2018. https://bitcointalk.org/index.php?topic=3256693.0.

———. 2018b. “Network Attack on XVG / VERGE (Page 57)”. Bitcointalk. 2018. https://bitcointalk.org/index.php?topic=3256693.msg38135174#msg38135174.

PTY X. 2018. “What is a Parallel Chain (Asset Chain)?” Komodo Platform. 2018. https://komodoplatform.atlassian.net/wiki/spaces/KPSD/pages/71729160/What+is+a+Parallel+Chain+Asset+Chain.

Quesnelle, Jeffrey. 2017. “On the linkability of Zcash transactions”. arXiv preprint arXiv:1712.01210.

Roberts, Jeff John. 2018. “Bitcoin Spinoff Hacked in Rare ‘51% Attack’”. FORTUNE. 2018. http://fortune.com/2018/05/29/bitcoin-gold-hack/.

Saberhagen, Nicolas Van. 2013. “CryptoNote v 2.0”.

Sasson, Eli Ben, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, en Madars Virza. 2014. “Zerocash: Decentralized anonymous payments from bitcoin”. In 2014 IEEE Symposium on Security and Privacy (SP), 459–74.