Wallet multi-sig e attacco informatico a Bitfinex (2016)

Saverio Mattia Merenda[1]

[1]saveriomattia.merenda@studenti.unipr.it

Questa relazione analizza l'attacco informatico del 2016 alla piattaforma di scambio di criptovalute Bitfinex, il quale rappresenta uno degli eventi più significativi nella storia delle criptovalute. Gli hacker rubarono ∼120k bitcoin, valutati ∼72 milioni di dollari all'epoca, sfruttando una vulnerabilità nella gestione dei wallet gestiti dalla piattaforma. Dopo l'attacco, i cybercriminali implementarono un complesso piano di riciclaggio, utilizzando tecniche di offuscamento, mixer e tumblers, e integrando i fondi nel sistema bancario tradizionale. Le indagini, condotte da diverse agenzie governative statunitensi, portarono all'arresto dei cybercriminali nel febbraio 2022, grazie alla scoperta di un file criptato contenente gli indirizzi dei wallet e le chiavi private. L'operazione di recupero dei fondi, valutati ∼3.6 miliardi di dollari nel 2022, rappresentò la più grande confisca finanziaria nella storia del Dipartimento di Giustizia degli Stati Uniti d'America.

Keywords: Cybercrime, Hack, Cryptocurrencies, Bitcoin, Bitfinex.

1 Introduzione

Nell'agosto 2016, Bitfinex, una delle principali piattaforme di scambio di criptovalute con sede a Hong Kong, fu colpita da un attacco informatico di vasta portata che scosse profondamente l'intero ecosistema delle criptovalute. Gli aggressori riuscirono a sottrarre 119756 bitcoin, che all'epoca avevano un valore complessivo di circa 72 milioni di dollari USA. Questa cifra rappresentava lo 0.75% dell'intera supply di bitcoin in circolazione al tempo, sottolineando l'enorme impatto dell'incidente sia in termini economici che di fiducia nel settore (Wikipedia, 2016). Questo evento è rimasto a lungo uno dei più gravi attacchi nella storia delle criptovalute fino a quel momento, segnando un punto critico per la sicurezza delle piattaforme di scambio.

L'attacco sfruttò una vulnerabilità legata alla gestione dei wallet multi-sig (multi-signature), una misura di sicurezza che teoricamente avrebbe dovuto proteggere gli asset degli utenti. Bitfinex utilizzava un'infrastruttura sviluppata in collaborazione con BitGo, un servizio di custodia che forniva firme aggiuntive per migliorare la sicurezza delle transazioni. Tuttavia, gli hacker riuscirono a bypassare queste protezioni compromettendo sia la piattaforma che la componente BitGo, dimostrando che anche le configurazioni avanzate erano vulnerabili a sofisticati attacchi (Bitbo, 2016; of Justice, 2016).

Le conseguenze dell'hack furono devastanti. Bitfinex sospese immediatamente tutte le operazioni e iniziò un'indagine per determinare come fosse stato perpetrato l'attacco. La notizia causò un crollo istantaneo del prezzo del bitcoin, che perse circa il 20% del suo valore, scendendo a circa 480 dollari prima di una graduale ripresa. Questo calo rifletteva non solo le perdite finanziarie dirette, ma anche il colpo alla fiducia degli investitori e degli utenti verso le piattaforme centralizzate di scambio.

La Figura 1 mostra l'evoluzione degli attacchi hacker nel settore crypto dal 2016 al 2022, evidenziando un aumento significativo sia nel valore sottratto (barre blu) che nel numero di attacchi (linea arancione). Se fino al 2019 i valori si mantenevano contenuti sotto i $2 miliardi, dal 2020 si è registrata una forte accelerazione che ha portato a un picco di quasi $4 miliardi rubati nel 2022. È interessante notare come il 2021 abbia registrato il maggior numero di attacchi, mentre il 2022, pur con meno incidenti, ha visto sottrarre il valore più alto, suggerendo una crescente sofisticazione delle tecniche utilizzate.

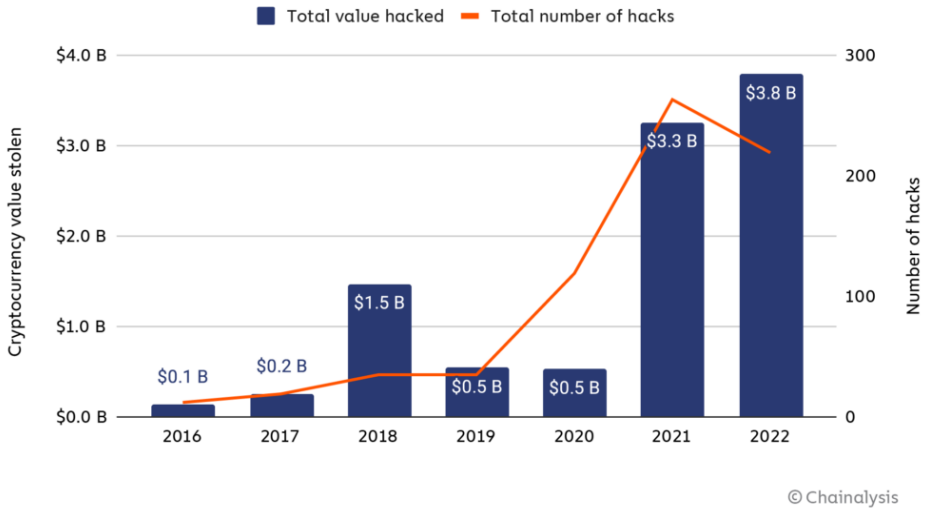

Figure 1: Valore totale rubato in attacchi informatici alle criptovalute, 2016–2022 (Chainalysis, 2024).

2 Wallet multi-sig

I wallet multisig (*multi-signature*) sono una tecnologia avanzata progettata per aumentare la sicurezza delle transazioni su blockchain. A differenza dei wallet tradizionali, che richiedono una sola chiave privata per autorizzare una transazione, i wallet multisig richiedono la partecipazione di più chiavi, rendendo più difficile per un attaccante ottenere il controllo totale sui fondi (Coindesk, 2016). Tuttavia, il caso di Bitfinex del 2016 dimostra che anche una tecnologia ben progettata può essere vulnerabile se configurata o gestita in modo non adeguato.

2.1 Funzionamento dei wallet multisig

Un wallet multisig opera secondo uno schema N-of-M, in cui N rappresenta il numero minimo di chiavi necessarie per autorizzare una transazione, mentre M è il numero totale di chiavi disponibili. Ad esempio, in una configurazione 2-of-3, una transazione richiede due chiavi su tre per essere valida. Questo meccanismo si basa su script che

operano direttamente sulla blockchain, definiti come script di *locking* e *unlocking*. Lo script di locking stabilisce le condizioni che devono essere soddisfatte per sbloccare i fondi, mentre lo script di unlocking include le firme necessarie per dimostrare che queste condizioni sono state rispettate.

I wallet multisig sono comunemente utilizzati in contesti dove la sicurezza è fondamentale. La distribuzione delle chiavi tra più entità riduce i rischi associati alla compromissione di una singola chiave. Per esempio, in uno schema 2-of-3, anche se una chiave viene compromessa, l'attaccante non può accedere ai fondi senza ottenere almeno un'altra chiave. Questo approccio è particolarmente utile in contesti aziendali, dove è necessario che più parti approvino una transazione, o come protezione contro la perdita di una chiave privata, poiché le chiavi rimanenti possono comunque garantire l'accesso.

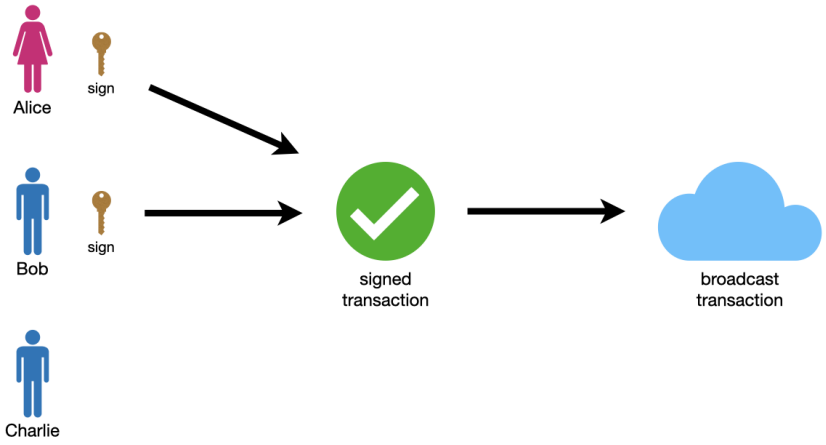

Figure 2: Esempio di transazione multisig 2-of-3.

2.2 Il caso di Bitfinex

Bitfinex utilizzava uno schema multisig 2-of-3 in collaborazione con BitGo, un provider di servizi di sicurezza blockchain. La configurazione prevedeva che una chiave fosse detenuta da Bitfinex, una da BitGo e una terza fosse conservata come backup offline. Per autorizzare una transazione, erano necessarie due firme: una da Bitfinex e una da BitGo.

Gli hacker riuscirono a compromettere questa configurazione sfruttando alcune debolezze chiave. Innanzitutto, riuscirono ad ottenere l'accesso alla chiave detenuta da Bitfinex compromettendo i suoi sistemi. Questo permise loro di generare richieste di transazione fraudolente, firmate con la chiave compromessa. Successivamente, queste richieste furono inviate a BitGo, che aveva implementato un sistema di approvazione automatica delle transazioni basato su criteri predefiniti. Purtroppo, tali criteri non erano abbastanza restrittivi da rilevare attività anomali. BitGo approvò quindi le transazioni, fornendo la seconda firma necessaria per trasferire i fondi agli indirizzi controllati dagli hacker.

Un altro fattore che facilitò l'attacco fu l'assenza di un monitoraggio efficace delle transazioni. Non furono rilevati comportamenti sospetti, come l'invio di un numero elevato di richieste di transazione in un breve periodo di tempo. Questo permise agli

attaccanti di completare il furto senza essere fermati. In particolare, la mancanza di un controllo manuale o di validatori addizionali rese possibile l'approvazione automatica di transazioni fraudolente da parte di BitGo, dimostrando che una configurazione multisig mal gestita può essere vulnerabile nonostante le sue premesse di sicurezza.

3 Riciclaggio dei fondi

Successivamente all'attacco, gli hacker identificati come Ilya Lichtenstein e Heather Morgan, intrapresero un elaborato piano di riciclaggio per occultare la provenienza dei ∼120k bitcoin rubati (Sun, 2024). Questa operazione, rivelatasi una delle più complesse mai documentate nel mondo delle criptovalute, mise in luce le vulnerabilità dei sistemi di sicurezza e le sfide legate al tracciamento dei fondi digitali. La coppia sfruttò la natura pseudonima delle transazioni su blockchain, combinandola con tecniche avanzate di offuscamento per rendere estremamente difficile il tracciamento dei bitcoin.

Lichtenstein, l'architetto principale dell'operazione, orchestrò il trasferimento dei fondi rubati attraverso più di 2.000 transazioni non autorizzate, utilizzando identità fittizie e strumenti informatici per automatizzare e frammentare i movimenti di denaro. Queste transazioni frammentavano i fondi in piccole quantità e li distribuivano su un vasto numero di wallet, complicando ulteriormente il loro tracciamento. L'uso di mixer e tumblers, strumenti progettati per offuscare la provenienza delle criptovalute, contribuì a mascherare il flusso di denaro, rendendo difficile distinguere i bitcoin rubati da quelli legittimi (Press, 2024).

Parte dei fondi fu trasferita su mercati del dark web, come AlphaBay, un marketplace illegale che facilitava il commercio anonimo di beni e servizi illeciti. Qui, i bitcoin furono scambiati per altre valute virtuali o utilizzati per acquistare beni e servizi che potessero essere rivenduti nel mondo reale per riciclare il denaro. Inoltre, la coppia di cybercriminali aprì conti aziendali negli Stati Uniti, utilizzando documenti falsi per legittimare le transazioni e integrare i fondi nel sistema bancario tradizionale.

La complessità del piano di riciclaggio rifletteva una strategia meticolosa e altamente sofisticata, ma non priva di falle. Nonostante l'uso di tecniche avanzate, l'immutabilità della blockchain, che registra ogni transazione in modo permanente, permise agli investigatori di tracciare il percorso dei fondi nel corso degli anni. Le autorità, collaborando con esperti di analisi blockchain, riuscirono a identificare schemi ricorrenti e a collegare indirizzi di wallet agli account creati da Lichtenstein e Morgan (Monde, 2024).

La Figura 3 mostra l'evoluzione delle principali piattaforme utilizzate per il riciclaggio di criptovalute tra il 2020 e il 2022.

4 Indagini

Le indagini sull'hack di Bitfinex furono il risultato di una complessa operazione condotta da diverse agenzie governative statunitensi, tra cui il Dipartimento di Giustizia (DoJ), l'FBI, l'IRS-Criminal Investigation (IRS-CI) e l'Immigration and Customs Enforcement-Homeland Security Investigations (HSI). La cooperazione tra queste agenzie evidenziò l'importanza di un approccio multidisciplinare per affrontare crimini finanziari di portata globale, che coinvolgevano non solo tecnologie avanzate, ma anche intricati schemi di riciclaggio transnazionali.

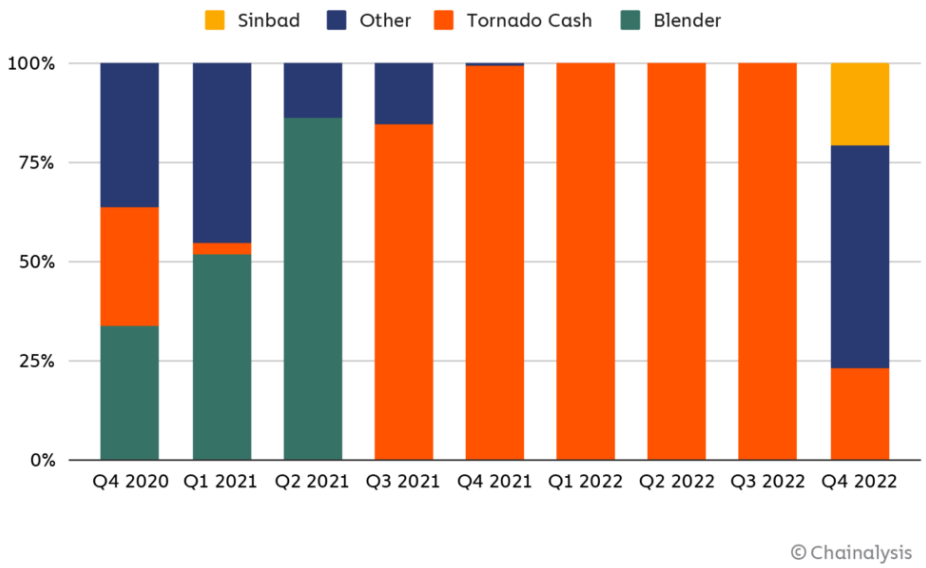

Figure 3: Piattaforme utilizzate per il riciclaggio di criptovalute, 2020–2022 (Chainalysis, 2024).

La svolta cruciale nelle indagini avvenne nel febbraio 2022, quando le autorità riuscirono ad arrestare Ilya Lichtenstein e Heather Morgan a New York. I due furono accusati di cospirazione per riciclare i fondi rubati e affrontarono accuse che potevano comportare pene detentive significative. L'arresto fu reso possibile grazie a un'indagine meticolosa che combinò analisi forense sulla blockchain con tradizionali tecniche investigative, come il monitoraggio digitale e il recupero di dati archiviati nel cloud.

Un elemento chiave dell'indagine fu la scoperta di un file crittografato archiviato nel cloud storage di Lichtenstein (i.e., Google Drive). Questo file conteneva un elenco dettagliato degli indirizzi dei wallet e delle chiavi private corrispondenti, direttamente collegati ai fondi sottratti durante l'hack di Bitfinex. Le chiavi private rappresentavano un accesso diretto ai bitcoin rubati, e il loro recupero permise alle autorità di sequestrare oltre 94K bitcoin, valutati circa $\sim$3.6 miliardi di dollari. Questa operazione segnò la più grande confisca finanziaria mai effettuata dal Dipartimento di Giustizia, nonché una pietra miliare nella lotta contro il crimine legato alle criptovalute (Press, 2024).

La scoperta del file criptato mise in evidenza l'importanza dell'archiviazione digitale e del tracciamento delle impronte elettroniche nelle moderne indagini criminali. Nonostante l'elaborata strategia di offuscamento messa in atto dagli hacker, le loro attività online, inclusa l'archiviazione dei dati sensibili nel cloud, lasciarono tracce che le autorità furono in grado di seguire. Questo episodio dimostrò che, nonostante l'anonimato e la pseudonimità delle criptovalute, l'immutabilità e la trasparenza delle blockchain possono essere utilizzate come strumenti potenti per risalire ai responsabili di attività illecite. L'operazione rappresentò anche un forte messaggio deterrente, evidenziando che i crimini nel mondo delle criptovalute non sono immuni all'azione delle autorità. La cooperazione tra diverse agenzie e l'uso di strumenti tecnologici avanzati confermarono l'impegno crescente nel contrastare i crimini finanziari digitali su scala globale.

5 Condanne e arresti

Ilya Lichtenstein e Heather Morgan furono accusati di cospirazione per riciclare i fondi rubati durante l'hack di Bitfinex, nonché di cospirazione per frodare gli Stati Uniti. Nel febbraio 2022, le autorità statunitensi avevano arrestato entrambi, con le accuse che li ponevano al centro di un'operazione globale di riciclaggio di denaro illecitamente ottenuto. Nel mese di agosto 2023, Lichtenstein e Morgan hanno ammesso la loro colpevolezza per il reato di cospirazione finalizzato al riciclaggio di denaro (Express, 2024).

I due furono condannati a cinque anni di reclusione federale, seguiti da tre anni di libertà vigilata. La loro sentenza rappresenta una delle pene più severe mai inflitte a cybercriminali coinvolti in attacchi legati alle criptovalute, evidenziando la fermezza delle autorità nel perseguire e punire i reati informatici.

La condanna di Lichtenstein e Morgan è considerata un importante traguardo nella lotta contro la criminalità informatica, soprattutto nel contesto delle criptovalute. Dimostra che le autorità governative hanno le risorse, la determinazione e la capacità di far rispettare la legge anche in contesti di criminalità complessa, caratterizzati da tecniche sofisticate di anonimizzazione e offuscamento. L'operazione non solo ha portato alla confisca di oltre 94K bitcoin, ma ha anche inviato un chiaro messaggio che i crimini legati alle criptovalute non rimangono impuniti e che la trasparenza e il tracciamento delle blockchain possono essere fondamentali nel portare giustizia.

References

Bitbo. Bitfinex hack 2016: 119,756 bitcoin stolen, 2016. URL https://calendar.bitbo.io/bitfinex-hack/. Accessed: 2024-12-18.

Chainalysis. The blockchain data platform, 2024. URL https://www.chainalysis.com/. Accessed: 2024-12-21.

Coindesk. What the bitfinex hack means for bitcoin multi-sig security, 2016. URL https://www.coindesk.com/markets/2016/08/05/what-the-bitfinex-hack-means-for-bitcoin-multi-sig-security/. Accessed: 2024-12-21.

The Cyber Express. 2016 bitfinex hack case closed: Ilya lichtenstein sentenced for laundering billions in stolen bitcoin, 2024. URL https://thecyberexpress.com/hack-of-bitfinex-for-laundering/. Accessed: 2024-12-18.

Le Monde. Vol de 120 000 bitcoins: prison ferme mais peines légères pour le couple responsable du piratage de bitfinex, 2024. URL https://www.lemonde.fr/pixels/article/2024/11/19/vol-de-120-000-bitcoins-prison-ferme-mais-peines-legeres-pour-le-couple-responsable-du-piratage-de-bitfinex_6402582_4408996.html. Accessed: 2024-12-18.

U.S. Department of Justice. 2016 bitfinex hack, 2016. URL https://www.justice.gov/usao-dc/2016-bitfinex-hack. Accessed: 2024-12-18.

Associated Press. Man who stole and laundered roughly $1b in bitcoin is sentenced to 5 years in prison, 2024. URL https://apnews.com/article/bb592f0f06cdd8c2854a1a2259660c70. Accessed: 2024-12-18.

The Sun. Who is heather morgan's husband ilya lichtenstein and how long was his bitfinex crypto theft jail sentence?, 2024. URL https://www.thesun.co.uk/news/17594836/heather-morgan-husband-ilya-lichtenstein/. Accessed: 2024-12-18.

Wikipedia. 2016 bitfinex hack, 2016. URL https://en.wikipedia.org/wiki/2016_Bitfinex_hack. Accessed: 2024-12-18.