

LE CRIPTOVALUTE COME STRUMENTO E TARGET DEL CYBERCRIME

In 3 sorsi – *L'introduzione delle criptovalute ha impattato notevolmente sull'evoluzione dei crimini informatici. Nonostante anonimità e decentramento facilitino la commissione di illeciti nel mondo digitale, le criptomonete costituiscono altresì il nuovo target del cybercrime.*

1. CRIPTOVALUTE E TECNOLOGIA BLOCKCHAIN

Le **criptovalute** sono mezzi di scambio digitale originatosi sulla rete internet e basate sui principi della crittografia, necessari per condurre e proteggere le transazioni. In tale sistema, ogni singola operazione si basa su un messaggio crittografato e firmato digitalmente, il quale indica il trasferimento di una certa somma di valuta ad un altro utente; successivamente, essa viene iscritta in un registro pubblico decentralizzato noto come **blockchain**. L'introduzione delle criptovalute risale al 2008, con l'annuncio in un paper accademico attribuito a Satoshi Nakamoto della creazione del **Bitcoin**, una versione puramente *peer-to-peer* del contante elettronico capace di inviare pagamenti online direttamente da un utente all'altro senza l'intermediazione di un'**istituzione finanziaria**. Se da un lato la creazione, la distribuzione e il controllo della moneta all'interno della società è convenzionalmente regolata dallo Stato e dalle Banche Centrali attraverso l'uso di **politiche monetarie** e precisi standard normativi, dall'altro lato le criptovalute sfidano la tradizionale convinzione che la pianificazione centralizzata sia preconditione per il funzionamento degli **scambi di denaro**.

2. CRIPTOVALUTE E CRIMINI CIBERNETICI

Secondo le più recenti statistiche sulla cybersicurezza, nel 2021 i costi economici dei **crimini informatici** ammontano a sei miliardi di dollari; entro il 2025, si stima che tale cifra raggiungerà i \$10,5 miliardi. A tal proposito, le criptovalute hanno svolto un ruolo fondamentale nell'evoluzione dei crimini cibernetici, emergendo sia come strumento che come target di attività illecite compiute nel mondo digitale. In particolare, le criptovalute facilitano direttamente il pagamento da parte delle vittime di attacchi di estorsione *denial of service* e *ransomware*, in una relazione cosiddetta "V2C- *victim-to-criminal*" con i criminali informatici.

Nonostante ciò, il futuro utilizzo di criptovalute come mezzo di riscatto appare incerto a causa della loro estrema **volatilità**, che ne determina successive importanti fluttuazioni in termini di valore.

Allo stesso modo, le criptovalute si sono confermate come principale **metodo di pagamento** "C2C- *criminal-to-criminal*" nel **commercio elettronico** di strumenti e servizi illeciti sul *dark web*. Il dark web è inoltre divenuto il teatro di un fenomeno relativamente nuovo concernente il **riciclaggio di denaro** cibernetico: esistono infatti servizi specifici di riciclaggio di criptovalute, che nel caso del bitcoin sono divenuti noti come "tumblers" e "mixers". In maniera analoga, gli scambi di criptovalute e i processori di pagamento non risultano essere immuni da attacchi informatici: attività di **hacking** sono di fatto volte ad acquisire la chiave privata che funge da password di un wallet virtuale in cui sono contenute le criptovalute, al fine di "aprire" virtualmente il portafoglio ed appropriarsi del suo contenuto.

3. CRIPTOMONETE ED INCENTIVO AL CYBERCRIME

Il **decentramento** delle criptovalute offre un'eccellente opportunità per i criminali informatici intenzionati a compiere attività illecite: livelli di regolamentazione intrinsecamente limitati e **l'assenza di un governo** da parte di un'autorità centrale impedisce infatti un effettivo monitoraggio delle transazioni. Sebbene sia possibile ritracciare il flusso di uno spostamento di valuta, la manca di un collegamento effettivo ad un indirizzo bancario ed elementi tali da indentificare l'identità degli utenti garantiscono tuttavia un elevato livello di **anonimà delle transazioni** e, di conseguenza, dei criminali informatici, prevenendone dunque l'identificazione. Lo scambio di criptovalute in una **rete globale** di computer permette infine transazioni immediate e completamente indifferenti alla collocazione fisica.