LUISS

Dipartimento di
Impresa e Management

Cattedra Regolazione finanziaria e Innovazione

FINTECH E METODI DI FINANZIAMENTO AL TERRORISMO DI MATRICE JIHADISTA

Prof.ssa Mirella Pellegrini

RELATORE

Ilaria Contato (248911)

CANDIDATO

Anno Accademico 2021/2022

Un ringraziamento particolare alla mia relatrice, Professoressa Mirella Pellegrini, che mi ha seguito nell'elaborazione della tesi e alla Dottoressa Adriana Piancastelli Manganelli, già dirigente della Polizia di Stato e presso la Presidenza del Consiglio dei Ministri, che mi ha messo a disposizione la Sua preziosa esperienza, offrendomi consigli fondamentali sulle modalità di trattazione di un tema tanto sensibile e importante quale quello del terrorismo internazionale.

Indice

Indice delle figure

Introduzione

L'era digitale sta plasmando un mondo che grazie alle continue innovazioni sembra non avere confini. Il nuovo contesto, che vede come protagonista il Bitcoin ha fatto emergere nel tempo opportunità e rischi: da un lato, trattandosi di un sistema sorto dopo la crisi del 2008, aveva l'ambizione di creare un meccanismo di svincolo della moneta dal controllo dello Stato e di dare vita ad un sistema decentralizzato in cui sono gli stessi utenti a controllarne il funzionamento, ma allo stesso tempo la possibilità di effettuare transazioni in modo anonimo e privo di tracciamento.

La natura decentralizzata e poco controllabile del sistema, rende Bitcoin un circuito che si presta ad attività illecite, tra le quali anche il finanziamento al terrorismo di matrice jihadista.

La nuova fase decentralizzata che il terrorismo islamico sta vivendo gli permette di non avere confini e di agire globalmente, servendosi, in questo contesto anomico, di un'importante strumento: Internet. Applicazioni di messaggistica istantanea, social media e siti web pro jihad, hanno un ruolo centrale nel favorire i terroristi non solo nel diffondere la propaganda, o nel reclutamento di nuove leve, ma anche nella richiesta di sostegno economico ai suoi seguaci, ovunque nel mondo.

Le organizzazioni jihadiste hanno cominciato a sollecitare donazioni in bitcoin ormai già da anni e ciò si è verificato, non solo grazie alla facilità con cui è possibile creare un portafoglio bitcoin ed effettuare transazioni, ma anche a causa di una assenza di regolazione del sistema.

Il fenomeno Bitcoin, infatti, è caratterizzato dalla mancanza di un quadro giuridico chiaro e definito, in grado di regolare le transazioni operate sulla piattaforma ed è proprio in questo vuoto normativo che si insinua il terrorismo, con lo scopo di aggirare il sistema bancario occidentale.

La presente analisi si pone l'obiettivo di trattare l'evoluzione della nuova tecnologia Bitcoin e le modalità con cui il legame tra terrorismo e tecnologia sia andato via via rafforzandosi nel corso del tempo, nonché di evidenziare il ruolo importante che il web e il fintech possono giocare nel favorire la causa *jihadista*.

Capitolo 1 – LE CRIPTOVALUTE, I BITCOIN E LA BLOCKCHAIN

1.1 Origini delle Criptovalute: la cultura Cypherpunk

I termini Bitcoin e Blockchain fanno ormai parte della quotidianità: si tratta di una tecnologia alla portata di tutti, ma di cui pochi realmente conoscono origini e significato. Un primo richiamo al concetto di criptovaluta risale agli anni '80, precisamente al 1982, anno in cui David Chaum, docente di Informatica all'università di Berkeley ed esperto di crittografia, pubblicò un paper intitolato "*Blind Signatures for Untraceable Payments"*. Egli ipotizzò una forma di firma digitale (le c.d. "*blind signatures"*), realizzabile tramite l'applicazione di una serie di algoritmi e la cui finalità era quella di consentire a un soggetto di nascondere un messaggio prima di firmarlo. Proprio David Chaum evidenziò la potenzialità di questo meccanismo se utilizzato nel campo dei sistemi di pagamento, in quanto attuabile attraverso la creazione di una forma di denaro digitale finalizzata a garantire la privacy dei cittadini.

Le idee di Chaum catturarono l'attenzione degli attivisti del movimento Cypherpunk, i quali le inserirono successivamente nel loro manifesto, firmato nel marzo 1993 da Eric Hughes e nel quale si legge: *"We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money.*

Cypherpunks write code. We know that someone has to write software to defend privacy, and since we can't get privacy unless we all do, we're going to write it. We publish our code so that our fellow Cypherpunks may practice and play with it. Our code is free for all to use, worldwide"[1].

Da questo estratto del manifesto si evince che l'obiettivo del movimento era quello di tutelare la privacy delle persone e svincolarsi dal controllo dello Stato. Lo stesso Chaum portò avanti le idee del movimento e fondò la società DigiCash al fine di realizzare la moneta elettronica eCash. Fu la prima impresa che, integrando la crittografia con la moneta, rese possibile la realizzazione di transazioni anonime con un sistema centralizzato. Era possibile concludere transazioni utilizzando un software proprietario, che consentiva di prelevare moneta da una banca utilizzando chiavi crittografiche. Sarà, in seguito, lo stesso principio su cui si baseranno le criptovalute. DigiCash fallì e venne chiusa nel 1999, in quanto non riuscì a raggiungere una base di utenti sufficiente a supportare le operazioni e inoltre non esistevano aspettative perché potesse diventare una moneta indipendente dalle istituzioni,

[1] Hughes E. (1993), "*Cypherpunk's Manifesto*", disponibile su: https://www.activism.net/cypherpunk/manifesto.html

in quanto eCash era un sistema centralizzato fortemente legato all'azienda DigiCash. Quindi, nonostante rispettasse il principio base rappresentato dalla privacy degli utenti, mancava ancora una caratteristica essenziale: la decentralizzazione, che avrebbe consentito di operare in modo completamente indipendente dalle istituzioni finanziarie [2].

Con DigiCash si fece un primo passo in avanti, ma ancora non bastava.

Durante gli stessi anni e precisamente nel 1997, un altro cypherpunk, Adam Back, stava ultimando Hashcash. Si trattava di un sistema che riusciva a risolvere il problema basilare dei progetti di denaro digitale, la doppia spesa, cioè la possibilità di creare dei file digitali che potessero essere copiati e utilizzati due o più volte. Il sistema di Back risultava però complicato, in quanto ogni unità di hashcash poteva essere utilizzata per una sola transazione e coloro che partecipavano al sistema dovevano creare delle nuove monete ogni volta che desideravano utilizzarle.

I progressi effettuati da Back furono poi ripresi e sviluppati da Wei Dai, il quale nel 1998 pubblicò un paper sulla *mailing list* dei Cypherpunks, nel quale sviluppò la sua idea di criptovaluta, alla quale diede il nome di B-money. Nel documento di Wei Dai si legge: *"A community is defined by the cooperation of its participants, and efficient cooperation requires a medium of exchange (money) and a way to enforce contracts. Traditionally these services have been provided by the government or government sponsored institutions and only to legal entities. In this article I describe a protocol by which these services can be provided to and by untraceable entities"* (Wei Dai, 1998)[3].

Wei Dai propose due protocolli diversi per realizzare il suo progetto. Il primo prevedeva una rete non rintracciabile, nella quale è possibile individuare mittenti e destinatari solo tramite chiavi pubbliche, esenti dalla identificabilità personale, e in cui ogni messaggio è firmato dal mittente e crittografato dal destinatario. B-money avrebbe funzionato in modo decentralizzato, ma come afferma lo stesso Wei Dai nel paper: *"One of the more problematic parts in the b-money protocol is money creation"* (Wei Dai, 1998)[4]. Il sistema, quindi, non permetteva ancora di risolvere il problema della doppia spesa. Il secondo protocollo prevedeva la creazione di una rete in cui i partecipanti si distinguevano tra utenti regolari e "server", i quali conservavano una copia dei registri. Il progetto ideato da Wei Dai, nonostante sembrasse innovativo, rimase solo teorico. B-money, Hashcash ed eCash sono tre monete mai entrate davvero in utilizzo, ma hanno contribuito al progresso che poi rese possibile la nascita di bitcoin.

---

[2] Signorelli A.D. (2018), Il tascabile: "*Le origini di Bitcoin*", disponibile su: https://www.iltascabile.com/scienze/origini-bitcoin/

[3] Dai W. (1998), *B-Money*, disponibile su: http://www.weidai.com/bmoney.txt

[4] Ibidem.

Sempre nel 1998 Nick Szabo presentò una sua idea di valuta digitale, denominata Bit Gold: l'idea fondamentale era riprodurre una versione digitale dell'oro. Il meccanismo prevedeva del lavoro da parte di "miner" per generarlo e la quantità sarebbe stata limitata e non assoggettata al controllo di un'autorità centrale. Esisteva comunque un pericolo nella realizzazione pratica, dato che tornava il fenomeno della *double spending*, il rischio di poter duplicare i dati creati. Per tale motivo anche Bit Gold rimase un'idea che non trovò implementazione. Nonostante ciò, il progetto di Nick Szabo è considerato il più diretto predecessore di Bitcoin.
La potenzialità di tutte queste idee fu sfruttata da Satoshi Nakamoto, il quale raccogliendo gli sviluppi effettuati negli anni, riuscì a progettare quella che oggi conosciamo come tecnologia *Blockchain*.

1.1.1 Differenza tra valuta e criptovalute

Al fine di comprendere le criptovalute, è necessario innanzitutto avere ben chiaro che prima dell'invenzione della valuta basata sulla tecnologia crittografica si distingueva tra: moneta "fisica" ed "elettronica". La moneta fisica è rappresentata dalle monete metalliche o dalle banconote ed è quella che utilizziamo tutti i giorni in modo anonimo. La moneta elettronica è invece immateriale e consente di effettuare i pagamenti anche non avendo a portata di mano la moneta fisica. La valuta possiede delle funzioni fondamentali:

- *Unità di conto*: la moneta è utilizzata per confrontare il valore di prodotti e servizi tra loro.
- *Riserva di valore*: la moneta può essere conservata nel tempo, se non utilizzata, per consumare beni e servizi.
- *Mezzo di pagamento*: la moneta consente di scambiare beni e servizi.

Definite le funzioni associate alla moneta è possibile evidenziare come la criptovaluta non possa considerarsi valuta o moneta, in quanto non è in grado di assicurare tali funzioni. È possibile però affermare che racchiude in sé i vantaggi del contante e della moneta elettronica, in quanto rappresenta un sistema di pagamento a distanza e garantisce una sorta di anonimato. La valuta virtuale nasce con l'obiettivo di svincolarsi dal classico sistema economico basato sulla supervisione di un'autorità centrale che emetta la moneta e tracci le transazioni. Nella logica di questo nuovo tipo di moneta, tali funzioni vengono svolte dagli stessi utenti attraverso l'algoritmo di funzionamento della Blockchain. Tale tecnologia si basa infatti su una "peer-to-peer network", nella quale non esiste un server centrale, ma tutti i computer collegati hanno accesso alle risorse comuni.
È più corretto equiparare le criptovalute a degli "asset", in quanto, a differenza della moneta emessa dalle Banche Centrali, le valute virtuali sono limitate e rappresentano un attivo per chi le possiede,

senza che vi sia una controparte in passivo, infine sono sovranazionali, spendibili solo se qualcuno le accetta come mezzo di scambio[5].

1.2 La nascita del Bitcoin

Era il 31 ottobre 2008 quando Satoshi Nakamoto, pseudonimo dietro cui si cela la vera identità di colui (o coloro) che inventò bitcoin, inviò alla sua mailing list un messaggio contenente un abstract in cui spiegava il concetto di una nuova moneta peer-to-peer digitale e il White paper con i dettagli tecnici del progetto. Questo documento è conosciuto come il "Protocollo Bitcoin".
In tale data venne solamente pubblicato il protocollo Bitcoin, ma non era ancora stata creata la Blockchain di Bitcoin, la quale, insieme ai primi 50 BTC (c.d. "genesis block"), nacque il 3 gennaio 2009, quando proprio Satoshi Nakamoto minò il primo blocco. Il secondo blocco fu minato solo sei giorni dopo, sempre da Nakamoto, in quanto voleva essere certo del corretto funzionamento del software funzionasse bene prima di rilasciare la prima versione del client Bitcoin; operazione effettuata il 9 gennaio 2009. Furono così creati i primi 100 BTC e il primo trasferimento in assoluto avvenne tra Satoshi Nakamoto e Hal Finney e fu di 10 BTC.
Nel 2009 non erano ancora state create piattaforme su cui scambiare i bitcoin, i quali non avevano quindi ancora un valore di mercato in dollari, ma era solo possibile inviarli da wallet a wallet o minare[6].
Il 22 maggio 2010 è avvenuto il primo pagamento in bitcoin della storia. Laszlo Hanyecz pagò due pizze con 10.000 BTC, cifra che oggi ha un controvalore di 570 milioni di dollari[7].
Ad oggi i bitcoin in circolazione sono 19 milioni e negli anni hanno subito notevoli mutamenti nelle quotazioni; infatti, nell'aprile 2011 la quotazione ha superato un dollaro, per raggiungere, nell'ottobre 2021, il picco di 66 mila dollari. Satoshi Nakamoto ha programmato un numero massimo di bitcoin che è possibile emettere, fissato a 21 milioni di unità. Ciò vuol dire che si è raggiunto il 90% e secondo le stime per l'emissione dei restanti 2 milioni ci vorrà ancora un secolo. Si prevede infatti che l'ultimo bitcoin sarà minato nel 2140. Ci vorrà così tanto tempo perché il progetto di Satoshi Nakamoto prevede un incremento della capacità computazionale che occorre per risolvere il problema crittografico per il mining.

---

[5] Fontana F. (2020), Rivista italiana dell'antiriciclaggio "*Criptovalute e rischi di riciclaggio*". Disponibile su: https://www.antiriciclaggiocompliance.it/app/uploads/2020/08/Fontana.pdf

[6] Il mining è il processo con cui si validano e registrano le transazioni tramite la risoluzione di problemi matematici.

[7] Cavicchioli M. (2021), The Cryptonomist, *"La storia di Bitcoin dalla nascita ad oggi"*, disponibile su: https://cryptonomist.ch/2021/05/09/storia-bitcoin/

Ad oggi, inoltre, il 20% dei bitcoin emessi sono andati persi, il che vuol dire che sono nascosti in rete e i proprietari hanno perso le credenziali per accedervi[8]. In questa percentuale rientrerebbero anche i bitcoin dello stesso Satoshi Nakamoto e si tratterebbe di 1,1 milioni di bitcoin, minati da lui stesso e che risulta non abbia mai utilizzato. Egli fece perdere le sue tracce nel 2011 quando trasferì i domini di proprietà ad alcuni membri della comunità Bitcoin e consegnò il codice sorgente a un suo collaboratore, Gavin Andersen.

1.2.1 White paper del Bitcoin

"I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party" (Nakamoto, 2008)*[9]*. È questa la prima frase che il 31 ottobre 2008 Satoshi Nakamoto scrisse nella mail che inviò alla The Cryptography Mailing List, procedendo poi con un elenco delle proprietà principali del progetto, come segue: *"The main properties:*

Double-spending is prevented with a peer-to-peer network.

No mint or other trusted parties.

Participants can be anonymous.

New coins are made from Hashcash style proof-of-work.

The proof-of-work for new coin generation also powers the network to prevent double-spending" (Nakamoto, 2008).

Nell'introduzione del paper Satoshi Nakamoto afferma che è necessario un sistema di pagamento elettronico che si basi su una prova crittografica e non più sulla fiducia, affinché le controparti possano negoziare fra di loro senza che si inserisca una terza parte di fiducia. Inoltre, il progetto propone una soluzione al problema della doppia spesa, che si risolverebbe con l'utilizzo di un server di marcatura temporale distribuito peer-to-peer utilizzando la proof-of-work, la quale consentirebbe di generare la prova computazionale dell'ordine cronologico delle transazioni. In questo modo il sistema rimarrebbe sicuro fino a quando i nodi onesti controllano collettivamente più potenza CPU rispetto ai nodi attaccanti.[10]

---

[8] Soldavini P. (2021), *"I bitcoin emessi sono il 90% del totale, il 20% è sparito per sempre"*, Il sole 24 ore, disponibile su:https://www.ilsole24ore.com/art/i-bitcoin-emessi-sono-90percento-totale-circa-20percento-e-sparito-sempre-AETWwp4

[9] Cit. Nakamoto S. (2008), *"Bitcoin P2P e-cash paper",* disponibile su: https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html

[10] Nakamoto S. (2008), *"Bitcoin: un sistema di moneta elettronica peer-to-peer",* disponibile su: https://bitcoin.org/files/bitcoin-paper/bitcoin_it.pdf

Bitcoin costituisce quindi un sistema di pagamento incentrato su una rete di consenso decentralizzata gestita dai suoi utenti; ciò vuol dire che non è posseduta da nessuno, ma sono gli stessi utenti che la controllano. Gli sviluppatori migliorano il software, ma non possono effettuare un cambiamento nel protocollo, in quanto gli utilizzatori possono scegliere liberamente quale software e quale versione usare. Si deduce quindi che la rete Bitcoin può funzionare correttamente solo se esiste un consenso tra tutti gli utenti.

Nel progetto elaborato da Satoshi Nakamoto ogni utente può possedere uno o più indirizzi Bitcoin a cui corrisponde una chiave privata e ad ogni indirizzo è associata una firma digitale, che consente di autenticare ogni transazione. Ogniqualvolta un utente trasferisce valuta, firma digitalmente un hash della transazione precedente e la chiave pubblica del proprietario successivo, aggiungendo poi le stesse alla fine della valuta. Con questo meccanismo colui che riceve un pagamento può verificare le firme digitali al fine di validare la catena di proprietà (Nakamoto, 2008).

Quando si esegue una transazione, questa viene segnalata a tutti i computer che fanno parte del network, i quali ne verificano la validità attraverso la consultazione del registro pubblico delle transazioni e, una volta confermata la spesa, questa viene registrata in una lista, con gruppi di transazioni recenti: i blocchi. La rete Bitcoin si basa quindi sulla condivisione di un registro pubblico, la Blockchain, la quale racchiude tutte le transazioni elaborate e consente di verificare la validità di ogni transazione eseguita. È quindi possibile affermare che è proprio la caratteristica della decentralizzazione di tale sistema a rendere la rete Blockchain sicura.

1.2.3 Vantaggi e svantaggi del bitcoin

Al fine di comprendere nel dettaglio le caratteristiche di questa nuova tecnologia, si elencano di seguito i vantaggi e gli svantaggi riscontrati nel sistema Bitcoin.

Vantaggi:

- *Libertà di pagamento*: agli utenti è consentito ricevere e inviare qualsiasi quantità di denaro, ovunque nel mondo e in qualsiasi momento, senza alcun tipo di limitazione.
- *Costi di transazione*: per ricevere bitcoin non sono previste commissioni e nel momento in cui si effettua una transazione, all'utente è data la possibilità di controllare la quantità di commissioni da utilizzare. Quindi, non essendovi una correlazione tra importo trasferito e commissioni, è possibile inviare un elevato numero di bitcoin allo stesso costo dell'invio di un solo bitcoin.
- *Bassa rischiosità nelle transazioni*: gli utenti sono tutelati, in quanto le transazioni, sicure e irreversibili, non necessitano di dati sensibili o informazioni personali del cliente.

- *Sicurezza e controllo decentralizzato*: gli utenti hanno un controllo completo sulle proprie transazioni e sono tutelati dal furto d'identità, in quanto non esiste una correlazione tra informazioni personali e transazioni. Il sistema Bitcoin inoltre permette di proteggere il denaro attraverso dei backup o criptando i dati.
- *Trasparenza e neutralità*: la tecnologia blockchain offre tutte le informazioni inerenti all'offerta di moneta, affinché chiunque possa avere la possibilità di verificarle e utilizzarle. Il protocollo Bitcoin è crittograficamente sicuro, caratteristica che non permette ad alcuna organizzazione e ad alcun utente di controllarlo o manipolarlo.

Svantaggi:

- *Grado di accettazione*: l'alfabetizzazione in materia di Bitcoin è ancora carente: dato dimostrato dal fatto che ancora poche aziende accettano i bitcoin. Nonostante il numero sia in crescita, rimane insufficiente per poter beneficiare degli effetti della rete.
- *Volatilità*: il valore dei bitcoin e il numero delle aziende che li utilizzano sono ancora esigui e ciò ha delle conseguenze in termini di variazione del prezzo. Il mercato di Bitcoin non è ancora maturo, quindi piccoli scambi, o attività speculative, influenzano in modo significativo il prezzo.
- *Sviluppo continuo*: Bitcoin è in fase di maturazione. Il software Bitcoin si trova alla versione beta ed ha ancora alcuni fattori incompleti in fase di sviluppo attivo.
- *Vulnerabilità dei servizi*: l'impossibilità di poter alterare il protocollo Bitcoin, rende sia quest'ultimo che la blockchain un sistema sicuro. Tuttavia, esistono delle problematiche inerenti ai servizi connessi, come, ad esempio, gli Exchange centralizzati, cioè piattaforme a cui i soggetti si rivolgono per scambiare le criptovalute. Queste ultime sono soggette a innumerevoli attacchi hacker.
- *Attività illegali*: esiste concretamente la possibilità che la rete Bitcoin venga utilizzata per implementare attività illegali. Le transazioni sono anonime, in quanto è possibile rintracciare la chiave pubblica, ma non la persona fisica che ha effettuato il pagamento o la vendita. Questo meccanismo potrebbe portare a costruire piattaforme in cui si svolgono attività illegali, offrendo beni e servizi in cambio di bitcoin[11].

Nonostante gli svantaggi appena elencati, le peculiarità innovative della tecnologia, quali la decentralizzazione, la trasparenza e gli algoritmi criptografici, assicurano un sistema protetto. Ed è proprio grazie a queste caratteristiche intrinseche del sistema, che alcuni utenti ripongono fiducia in Bitcoin.

[11] Bitcoin.org, disponibile su: https://bitcoin.org/it/faq#cos-e-bitcoin

1.3 Caratteristiche tecniche: natura e funzionamento della tecnologia Blockchain

L'intera struttura grazie alla quale è possibile utilizzare i bitcoin è rappresentata dalla tecnologia Blockchain.

Prima di approfondire in concreto il significato di questa tecnologia è necessario fare una precisazione riguardo alle modalità di scrittura dei termini Blockchain e Bitcoin. "Blockchain", con l'iniziale maiuscola, rappresenta la tecnologia alla base dei Bitcoin, mentre "blockchain", con l'iniziale minuscola, indica l'architettura tecnologica alla base di altri sistemi, nei quali il criptoasset non è il Bitcoin. Il termine "Bitcoin" invece viene utilizzato con l'iniziale maiuscola quando si vuole far riferimento alla tecnologia e al protocollo di rete, mentre si scrive con l'iniziale minuscola quando ci si riferisce alla criptovaluta in sé.

1.3.1 Cos'è una Blockchain

La Blockchain è "una tecnologia in cui esiste un database di transazioni condiviso tra più nodi di una rete, validato dalla rete stessa e strutturato a blocchi (una catena di blocchi che contengono più transazioni). Le principali caratteristiche del database sono:

- Tracciabilità da tutti i partecipanti alla rete;
- Immutabilità e sicurezza attraverso sistemi crittografici." (Garavaglia R., 2018)[12]

Descrivere la Blockchain e il suo funzionamento è un processo complicato e, al fine di agevolarlo, è necessario comprenderne i principali termini tecnici, dei quali si riporta di seguito un elenco:

Criptoasset: sono i Bitcoin che rappresentano l'asset nativo nella Blockchain.

Nodo: il partecipante alla Blockchain.

Transazione: si ha nel momento in cui i nodi effettuano tra di loro scambi di criptoasset. Viene definita "verificata" quando è appunto stata verificata dai nodi partecipanti, mentre si definisce "validata" quando la transazione verificata si trova in un blocco validato. Allo stesso modo si definisce confermata, quando si tratta di una transazione verificata, che si trova in un blocco validato, distante dall'ultimo blocco validato di almeno cinque posizioni.

Blocco: è un raggruppamento di transazioni verificate.

Ledger: è il registro pubblico distribuito, nel quale vengono inserite sequenzialmente tutte le transazioni effettuate.

[12] Cfr. Garavaglia R. (2018), "*Tutto su Blockchain: capire la tecnologia e le nuove opportunità*", Ulrico Hoepli Editore S.p.A., Milano.

Hash: la funzione di Hash è un sistema matematico che converte un messaggio di lunghezza arbitraria in un messaggio in codice alfanumerico di lunghezza fissa, Digest o impronta digitale.

Difficoltà: equivale alla misura di quanto sia complicato trovare un Hash al di sotto di un certo target (tempo necessario per validare 2.016 blocchi). Non può essere inferiore a 1 e viene aggiustata in media ogni 12 giorni, ossia ogni 2.016 blocchi.

Mining: è il processo con cui si validano e registrano le transazioni e il nodo che pone in atto questa azione è definito "miner".

Proof-of-Work (PoW): è la prova utilizzata dai miner per dimostrare ai nodi la validazione del blocco.

Reward (ricompensa): rappresenta la remunerazione dei miner in criptoasset.

Mance (commissioni): costituiscono un incentivo al lavoro di validazione compiuto dai miner e possono essere liberamente incluse nelle transazioni.

Network: è costruito su un sistema di tipo P2P (Peer-to-Peer). La rete è distribuita, decentralizzata e paritaria.

Wallet: rappresenta un portafoglio elettronico nel quale sono memorizzate tutte le credenziali per accedere, spendere e trasferire criptoasset.

Firma digitale: è un processo crittografico basato su chiavi asimmetriche con la finalità di verificare che una transazione in Bitcoin sia realizzata dal possessore del wallet. Il proprietario del wallet possiede due chiavi, una privata e una pubblica. La chiave privata si compone di un codice alfanumerico associato a ogni wallet. La chiave pubblica è rappresentata dall'Address.

Illustrati i principali termini tecnici, è possibile ora esaminare come si sviluppa una transazione sulla Blockchain.

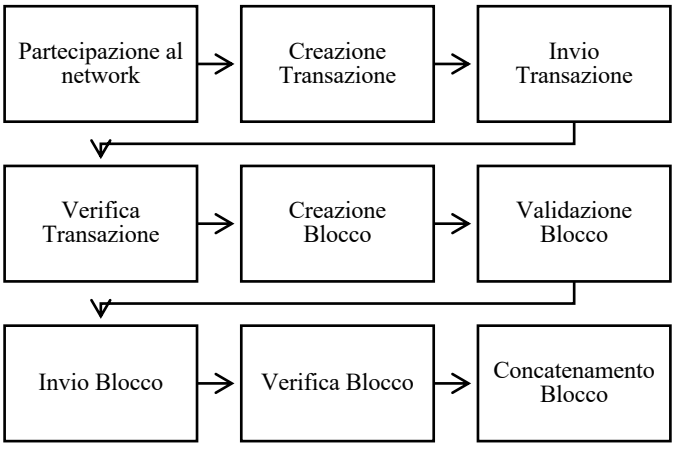

Figura 1– Ciclo di vita di una transazione sulla Blockchain[13]

[13] Cit. "*Tutto su Blockchain: capire la tecnologia e le nuove opportunità*", Ulrico Hoepli Editore S.p.A., Milano.

La Blockchain è quella struttura che permette di scambiare criptoasset attraverso le transazioni tra i partecipanti. Come illustrato nella figura sopra riportata, il processo ha inizio con la creazione di una transazione, la quale viene firmata digitalmente al fine accertare l'autorizzazione a spendere dei criptoasset. La transazione inviata al network viene sottoposta a verifica da parte dei nodi, i quali la diffondono a tutti gli altri e solo successivamente un nodo miner, che valida la transazione, la include in un blocco di transazioni che viene registrato sulla Blockchain.

La transazione registrata verrà infine stabilmente concatenata al blocco solo dopo essere stata confermata da un sufficiente numero di blocchi. Precisamente, l'approvazione deve provenire dal 50% più 1 dei nodi.

La Blockchain funziona secondo il meccanismo appena descritto perché, come anticipato nel paragrafo precedente, non è un sistema centralizzato, bensì un database distribuito che si basa sulla tecnologia peer-to-peer, un sistema di verifica aperto, che permette al sistema Bitcoin di funzionare senza l'intermediazione di istituti di credito per eseguire una transazione, in quanto ogni nodo possiede una copia del ledger sincronizzata localmente. Quindi, affinché una transazione possa essere eseguita correttamente, è necessario seguire un procedimento ben preciso.

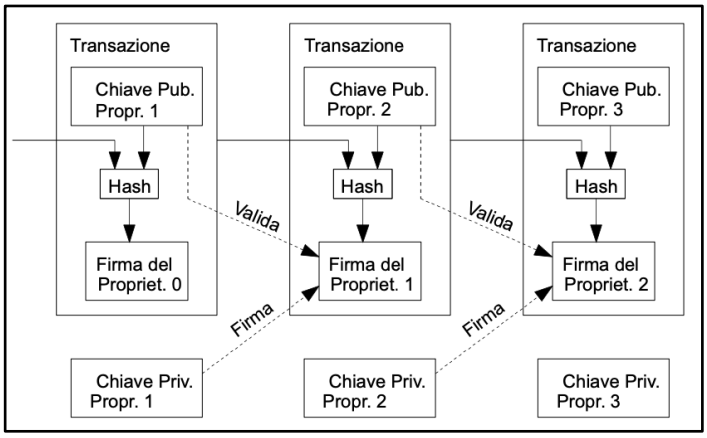

Figura 2– La struttura delle transazioni[14]

Il nodo che crea una transazione, prima di poterla inviare agli altri nodi, esegue il seguente processo:

1. Attraverso la funzione di Hash crea il Digest della transazione;
2. Per ottenere la firma digitale della transazione, utilizza la chiave privata del mittente per firmare il Digest;
3. Infine, inserisce la chiave pubblica del destinatario.

Terminato questo procedimento, il destinatario riceverà la transazione e per decifrare la firma digitale e ottenere il Digest dovrà utilizzare la chiave pubblica del mittente. L'autenticità della transazione

[14] Cfr. https://bitcoin.org/files/bitcoin-paper/bitcoin_it.pdf

viene confermata solo nel momento in cui, applicando la funzione di Hash alla stessa, sarà possibile confrontare il risultato del Digest creato dal mittente e appurare che i due valori coincidano. La chiave pubblica posseduta dal destinatario è utile nel caso in cui quest'ultimo decida di spendere i criptoasset ricevuti dal mittente.

L'utilizzo del meccanismo della firma digitale, basato sul processo crittografico su chiavi asimmetriche, permette di garantire la legittimità della transazione, in quanto, qualora il destinatario della stessa non fosse chi dice di essere e cercasse di utilizzare la disponibilità trasferita dal mittente, non potrebbe usare la propria chiave privata per firmare la transazione, a beneficio di un altro destinatario. Ciò avviene perché i criptoasset sono bloccati sul vero Address del destinatario e solo a quest'ultimo, con la propria chiave privata, è consentito sbloccarla.

In questo sistema innovativo, quindi, non esiste il concetto di conto, ma quando si esegue una transazione viene trasferito valore da un Input a un Output, ai quali non è associato né un conto né un'identità, ma solo le chiavi pubbliche dei partecipanti.[15]

1.3.2 L'attività di mining e la Proof-of-Work

La rete Bitcoin è considerata sicura in quanto l'intero sistema si basa sulla Proof-of-Work, la quale consente di generare la prova computazionale dell'ordine cronologico delle transazioni.

Il network è costituito da un numero elevatissimo di nodi, alcuni dei quali vengono chiamati nodi validatori o "miner", i quali effettuano la convalida delle transazioni. Il processo di validazione, anche chiamato "mining", ha inizio nel momento in cui un nodo riceve una transazione verificata e costruisce un blocco.

L'attività di mining può essere avviata da qualsiasi nodo validatore, che decide di candidarsi per gareggiare con altri nodi validatori alla presentazione della Proof-of-Work. Il vincitore, ossia il miner che riesce a dimostrare la Proof-of-Work validando il blocco, riceverà la reward, ovvero la ricompensa. La transazione introdotta dal miner vincitore rappresenta la prima transazione in ogni blocco e prende il nome di "coinbase".

Partecipare al mining significa competere con altri nodi per generare un hash di chiusura di ciascun blocco. Per generare l'hash, i miner devono risolvere un problema matematico che, oltre ad essere molto complicato, è lungo e costoso dal punto di vista dell'utilizzo dell'energia elettrica, indispensabile per supportare i server e la loro potenza computazionale.

[15] Cit. "*Tutto su Blockchain: capire la tecnologia e le nuove opportunità*", Ulrico Hoepli Editore S.p.A., Milano.

La difficoltà di questo processo si riscontra nel trovare un hash al di sotto di un determinato obiettivo, conseguentemente se la difficoltà è elevata, sarà necessaria più potenza di calcolo per estrarre lo stesso numero di blocchi.
Il compito dei nodi è trovare questo valore, definito "nonce", che una volta aggiunto alle altre transazioni, permette di ottenere il risultato richiesto. Il miner che diffonde la Proof-of-Work potrà ricevere la ricompensa per il lavoro di validazione, solo quando gli altri nodi avranno verificato la correttezza, è questo il meccanismo di consenso distribuito.

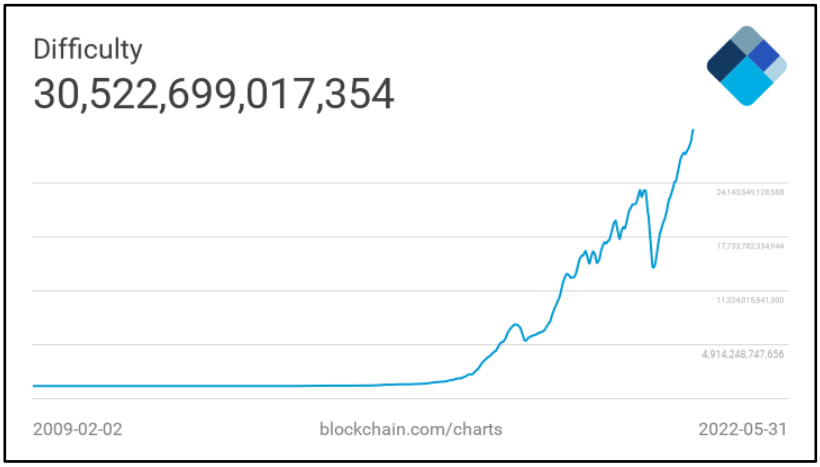

Figura 3 - Difficoltà del Network al 31/05/2022 (Fonte: blockchain.info)[16]

La struttura della Blockchain, organizzata per blocchi contenenti transazioni che formano una catena sequenziale marcata temporalmente, ha lo scopo di tutelare tutte le operazioni che vi hanno luogo. Il processo è quindi finalizzato alla tutela dell'integrità del sistema e viene stabilito per rendere difficile la modifica o la cancellazione delle informazioni validate. È un sistema che mira a prevenire le condotte tese alla creazione di transazioni false o all'alterazione dei blocchi.

1.3.3 L'offerta di bitcoin

Come menzionato precedentemente l'offerta di bitcoin è limitata e predefinita nel protocollo Bitcoin a 21 milioni, ciò significa che l'emissione si fermerà una volta raggiunta tale quantità. Non esiste un'autorità che controlli l'emissione, ma il meccanismo è gestito da un algoritmo e l'attività di mining rappresenta l'unica modalità con cui è possibile emettere nuovi bitcoin.
Il protocollo Bitcoin è stato progettato per creare nuovi bitcoin a una velocità fissa ed è proprio questo meccanismo che rende il mining un'attività altamente competitiva. Sono creati a un tasso decrescente

[16] Cfr. https://www.blockchain.com/charts (31/05/2022)

e prevedibile, un numero che si dimezza nel tempo, fino al raggiungimento di 21 milioni di bitcoin.[17] Tale tecnologia possiede un sistema che permette di dimezzare automaticamente il numero di nuovi bitcoin emessi ogni 210.000 blocchi, ovvero circa una volta ogni quattro anni e quindi, allo stesso modo, anche la ricompensa viene dimezzata nel medesimo arco temporale. Nel 2008, la ricompensa per ogni validazione ammontava a 50 BTC; già nel 2012 era diminuita a 25 BTC; nel 2016 è arrivata a 12,5 BTC e dal 2021, i minatori ricevono 6,25 BTC all'estrazione di un nuovo blocco. Il prossimo dimezzamento dovrebbe avvenire nel 2024, quando il premio scenderà a 3.125 BTC per blocco. Seguendo tale ragionamento e ipotizzando che la domanda rimanga elevata, l'acquisto sarà sempre più competitivo, proprio perché i bitcoin in circolazione nel mercato diminuiscono nel tempo. Le stime prevedono che quando sarà estratto l'ultimo bitcoin nel 2140, la ricompensa dei miners sarà data solo dalle commissioni applicate sulle transazioni.

Ad oggi ogni bitcoin è composto da cento milioni di satoshi, che rappresenta l'unità più piccola di bitcoin ed è chiamata così in onore del suo inventore. Ciò rende i bitcoin divisibili fino a otto cifre decimali; di conseguenza, chiunque ha la possibilità di acquistare una frazione di bitcoin con un minimo di un dollaro USA.

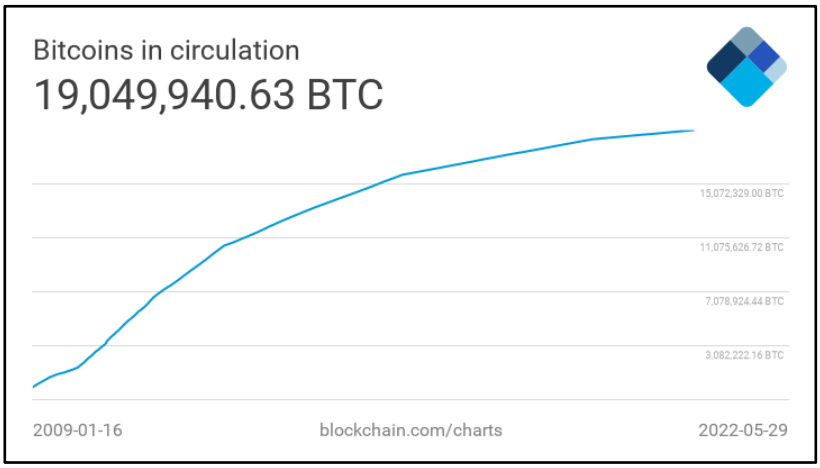

Figura 4– Totale Bitcoin in circolazione al 29/05/2022 (Fonte: blockchain.info)[18]

[17] Cfr. Bitcoin.org, disponibile su: https://bitcoin.org/it/faq#generale

[18] Cfr. https://www.blockchain.com/charts (29/05/2022)

Capitolo 2 – IL TERRORISMO ISLAMICO E IL SUO FINANZIAMENTO

Nel capitolo precedente sono stati presi in esame la nascita del sistema Bitcoin e il funzionamento della tecnologia alla base dello stesso, la Blockchain.
Si proseguirà, nel terzo capitolo, ad approfondire le potenziali connessioni, alcune sperimentate, tra criptovalute e sistemi criminali. Alcune delle caratteristiche proprie della valuta (quali l'assenza di un'autorità centrale e la difficoltà nel tracciamento dovuta alla pseudo-anonimità) rendono tale tecnologia uno strumento che si può prestare ad attività illecite. Le operazioni criminali che si avvalgono della criptovaluta sono molteplici e possono essere riassunte in: compravendita di materiale illecito, cybercrime, money laundering, pratiche di riciclaggio di denaro e forme di finanziamenti. In questa sede, però si approfondirà maggiormente il legame con il finanziamento al terrorismo.
È prima opportuno illustrare brevemente il termine terrorismo, sia le tecniche di finanziamento tradizionali di cui si avvale, per affrontare infine il tema delle nuove tecnologie.

2.1 L'ideologia dello Stato Islamico

Il 29 giugno 2014 Abu Bakr al-Baghdadi annuncia la nascita di uno Stato assolutista jihadista "su 250.00 chilometri quadrati di territorio strappati a Siria e Iraq"[19], con l'obiettivo di travolgere l'Islam e la comunità degli infedeli. È conosciuto con il nome di Stato Islamico ed è sorto nella regione del Tigri e dell'Eufrate con lo scopo di creare una "società perfetta", di generare "musulmani nuovi" e capaci di "purificare la Terra". Il leader, il Califfo, vuole raggiungere obiettivi ben precisi: unificare l'Islam sotto il dominio sunnita, eliminare gli sciiti, conquistare Roma che, nel sistema di propaganda, equivale a combattere e sconfiggere gli "infedeli" del mondo occidentale, che fanno capo alla "Città eterna" e imporre ovunque il rispetto della legge islamica.
Il Califfato è conosciuto soprattutto per metodi e prassi di violenza utilizzati per realizzare il progetto di unificare la comunità dei fedeli al fine di far riemergere al-Sham[20].
Il primo movimento che ha sostenuto l'uso della violenza per ristabilire lo stile di vita fondamentalista e ortodosso dei primi credenti islamici è stato quello dei Fratelli Musulmani, fondato nel 1928 in Egitto da Hasan al-Banna: che sono stati i primi a sostenere la necessità di ricostruire il Califfato dopo la dissoluzione dell'ultimo, quello ottomano, avvenuta nel 1924.

[19] Molinari M. (2015), *"Jihad: guerra all'occidente"*, RCS Libri Editore S.p.A., Milano.

[20] Parola che indica l'area che comprende i territori di Iraq, Siria, Giordania, Libano, Israele e Palestina.

La creazione degli Stati arabi tramite il disegno di confini artificiali è stata vissuta come un'imposizione delle potenze coloniali, con lo scopo di dividere la *umma*[21]. Per tale motivo il movimento si è avvicinato a lotte di liberazione, come le rivendicazioni territoriali palestinesi e la rivoluzione iraniana, realizzando l'obiettivo reale nel corso della guerra russo-afghana, apoteosi della pratica dell'odio contro l'Occidente. Fu proprio durante la guerra in Afghanistan che nacque Al-Qaeda, movimento fondato da Osama Bin Laden nel 1988 al fine di contrastare l'occupazione sovietica. Nel 2006 il gruppo iracheno dello Stato Islamico dell'Iraq e della Siria (ISIS), il cui leader era Abu Bakr al-Baghdadi, si proclama successore di Al-Qaeda in Iraq, per allargarsi fino alla Siria con la guerra civile. L'obiettivo di Osama bin Laden era spingere l'America a ritirarsi dal Medio Oriente, mentre al-Baghdadi desiderava trasformare la guerra santa realizzando uno Stato, retto dal potere assoluto della sharia[22] nel nome del successore di Maometto. Il fattore comune tra al-Qaeda e lo Stato Islamico è la matrice unica jihadista.

L'obiettivo globale è tornare alle origini dell'Islam, quando i confini delle conquiste di Maometto erano in continua espansione e all'interno non esistevano separazioni territoriali.

Abu Bakr al-Baghdadi dichiarò la nascita del Califfato jihadista con un editto che ne determinava l'estensione da Aleppo, in Siria, alla periferia di Baghdad, in Iraq.

L'organizzazione fondata nel 2013 con il nome di Stato Islamico dell'Iraq e del levante evolve in Stato Islamico (IS).

Il leader dello Stato islamico, per definirsi, utilizza la parola "Califfo", termine che per i musulmani osservanti ha un grande valore: "*Khalifa"* significa "successore" di Maometto, che può legittimamente chiedere fedeltà a tutti i musulmani, con riferimento storico alle origini dell''Islam, al profeta Maometto e ai quattro "califfi giusti", che riuscirono a guidare i musulmani ed espandere il regno dell'Islam.

"Baqiyya wa Tatamaddad", è questa la frase che più rappresenta lo Stato Islamico il cui significato è restare ed espandersi in continuazione[23]. Restare, nel senso di resistere ai nemici, ed espandersi nel significato di allargare i confini ed imporre la sharia a nuove popolazioni.

La nascita del Califfato rappresentava per Abu Bakr al-Baghdadi un progetto di unificazione dell'Islam sunnita, ma l'aspirazione non si ferma qui perché l'obiettivo ideologico finale restano la

[21] Nell'islam il termine umma si riferisce alla comunità dei fedeli.

[22] Nell'Islam la sharia rappresenta il complesso di regole di vita e di comportamento dettato da Dio per la condotta morale, religiosa e giuridica dei suoi fedeli.

[23] Vidino L., Marone F., Entenmann E. (2017), *"Jihadista della porta accanto: radicalizzazione e attacchi jihadisti in occidente",* ISPI, disponibile su:
https://www.ispionline.it/sites/default/files/pubblicazioni/report_jihadista_della_porta_accanto.pdf

conquista di Roma e la realizzazione di una jihad globale. La conquista della capitale del cristianesimo rappresenterebbe simbolicamente la vittoria decisiva contro gli infedeli[24].

2.1.1 Il concetto di Jihad

Il fondamentalismo islamico viene identificato nel termine jihadismo. Quest'ultimo è un elemento centrale dell'islam, nonostante non rientri formalmente tra i cinque precetti fondamentali[25]. Letteralmente il termine jihad può essere tradotto come "sforzo"[26], interpretato nel senso di miglioramento del credente, che si estende anche al combattente per la causa sacra, definito "*mujahid"* (colui che porta avanti lo sforzo).

Nonostante il jihad si sostanzi nel combattimento, deve essere inteso in senso difensivo, in quanto nel Corano è suggerito di combattere "coloro che vi combattono", "senza eccessi". Tale visione non è condivisa in modo unanime, in quanto diversi hadith, brevi narrazioni in cui viene espresso il pensiero e l'insegnamento del Profeta Maometto, inducono a letture più violente del jihad, da intendere come vera e propria lotta fisica.

Il fondamentalismo islamico promuove il jihad contro coloro che sono considerati infedeli[27], dato che, come specificato in precedenza, lo scopo dei gruppi jihadisti è creare uno stato islamico governato dalla legge islamica, la sharia. L'Europol definisce il jihadismo come "un'ideologia violenta, che si serve dei concetti tradizionali islamici. I jihadisti legittimano l'uso della violenza con richiamo alla dottrina islamica tradizionale sulla jihad, un termine che significa letteralmente "lotta" o "sforzo", ma nella legge islamica è considerata guerra santa".

Al-Qaeda e lo Stato Islamico sono i maggiori rappresentanti dei gruppi jihadisti.

---

[24] Molinari M. (2015), *"Il califfato del terrore: perché lo stato islamico minaccia l'occidente"*, RCS Libri Editore S.p.A., Milano.

[25] I cinque pilastri dell'Islam rappresentano gli obblighi fondamentali previsti dalla legge religiosa, la sharia, per ogni credente musulmano e sono: la testimonianza di fede (shahādah), la preghiera (ṣalāt), l'elemosina legale (zakāt), il digiuno (ṣawm) nel mese di Ramadan, il pellegrinaggio (ḥajj) alla mecca.

[26] Roy O. (2017), "Generazione ISIS: chi sono i giovani che scelgono il califfato e perché combattono l'occidente", Feltrinelli Editore Milano.

[27] Enciclopedia Treccani, *"jihadismo",*disponibile su: https://www.treccani.it/enciclopedia/jihadismo/

2.2 I canali di finanziamento

La capacità di un'organizzazione terroristica di raggiungere i propri obiettivi è determinata anche dalla quantità di risorse a disposizione. Le risorse finanziarie hanno lo scopo di coprire sia i costi degli attacchi e la logistica, ma anche le spese per garantire, nel tempo, il sostentamento stesso dell'organizzazione.

I fondi necessari per le attività terroristiche sono in apparenza relativamente esigui rispetto all'immaginario generale: per esempio, gli attentati dell'11 settembre 2001, hanno avuto un costo complessivo di circa 500 mila dollari, importi facilmente reperibili dalle cellule terroristiche[28]. Le risorse finanziarie, quindi, non sono finalizzate solamente a sostenere le singole attività, ma devono garantire il mantenimento nel tempo dell'intera organizzazione ed è questo il motivo per cui sono necessarie sostanziose e regolari fonti di finanziamento. I finanziamenti per l'operatività di queste organizzazioni derivano da molteplici fonti, provenienti sia da canali illegali, che legali.

Le tipologie di finanziamento sono numerose e differenziate, quali: presunte attività di contrabbando di petrolio, di traffico di armi, di migranti, di esseri umani e di organi, la pirateria, il traffico di stupefacenti e di medicinali. Tra le presunte attività illecite anche il contrabbando di sigarette, il traffico di antichità, i traffici illeciti sul dark web, il riciclaggio e lo sfruttamento illegale di money transfer e criptovalute, le rapine, le estorsioni e l'imposizione di tasse di vario tipo nelle aree controllate.

Le principali organizzazioni terroristiche utilizzano diverse modalità di finanziamento.

Al-Qaeda, per esempio, sembra dedicarsi al trading di petrolio, ad attività quali la pirateria e il traffico di droga. Inoltre, importanti sembrano essere i finanziamenti provenienti dalla raccolta di fondi nelle moschee più radicali, nonché le risorse indirizzate alle ONG di carità islamica, le donazioni dei miliardari arabi, il riciclaggio di denaro, i presunti proventi dal riscatto del rapimento di ostaggi, i fondi derivanti da banche islamiche di investimento, come la Shari'a Banks.

Lo Stato Islamico (IS), dal canto suo, sembra reperire i finanziamenti attraverso rapimenti, estorsioni, rapine, imposizione di diverse forme di tasse nei territori di riferimento, vendita di petrolio e gas sul mercato nero, vendita di armi, traffico di donne e bambini come schiavi, traffici di oro e di opere d'arte rubate. Negli ultimi anni però, a causa delle sconfitte subite in Siria e in Iraq, sono diminuiti i finanziamenti provenienti da queste aree e soprattutto quelli provenienti dal petrolio. Per questo lo Stato Islamico ha iniziato ad utilizzare nuove tipologie di finanziamento e ad investire in attività

[28] Palumbo G. (2011), *Hawala e Finanza. Le vie segrete del denaro nell'era dell'economia globale,* Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali – CSSII, disponibile su: https://www.cssii.unifi.it/upload/sub/hawala-e-finanza-islamica-cssii.pdf

commerciali legittime, come il settore alberghiero, le case di cura e le attività agricole[29], cercando di connotare, almeno in apparenza, schemi socialmente accettabili.

2.2.1 Il finanziamento apparentemente "lecito"

Tra il 2013 e il 2014 lo Stato Islamico ampliò il numero dei territori occupati, che, sotto il controllo delle organizzazioni terroristiche vengono sottoposti a imposte territoriali, contribuendo a rimpinguare le casse delle organizzazioni medesime[30].

È possibile distinguere tre tipi di imposte. La prima prende il nome di *kharāj*, un'imposta fondiaria islamica, riscossa dai proprietari terrieri e la cui aliquota è del 10%. La seconda imposta, che prevede una aliquota del 20%, è la *ghanîma*, una tassa su tutti quei beni che rappresentano bottini di guerra dei *mujaheddin*[31]. Da ultimo vi sono la *zakāt*, l'elemosina obbligatoria rituale e la *sadaqa*, l'elemosina opzionale.

"Le elemosine sono per i bisognosi, per i poveri, per quelli incaricati di raccoglierle, per quelli di cui bisogna conquistarsi i cuori, per il riscatto degli schiavi, per quelli pesantemente indebitati, per il sentiero di Allah e per il viandante. Decreto di Allah! Allah è saggio, sapiente"

(Surat Al-Tawbah 9:60).

Da questo estratto del Corano, in cui sono elencati i soggetti a cui dovrebbe essere destinato la *zakāt*, si comprende come la tassa non rappresenti né carità né un atto volontario, bensì un dovere religioso. L'imposta prende il nome di *zakāt* che letteralmente significa "purificazione" e ha il fine di purificare il cuore dall'avidità. Il fedele, quindi, versa il tributo dell'elemosina rituale sia al fine di purificare la propria ricchezza, che allo scopo di adempiere ad obblighi fondamentali previsti dalla legge religiosa, identificabili nei cinque pilastri dell'Islam.

Uno dei modi attraverso cui i terroristi acquisiscono la zakāt è attraverso l'operato delle Shari'a Banks. Si tratta di banche islamiche, privilegiate dai terroristi, in quanto non vi è possibilità di tracciare le somme devolute in favore della zakāt, trattandosi di operazioni non registrate nei bilanci

[29] Garofalo D. (2020), Analytica for intelligence and security studies: "*Il finanziamento del terrorismo jihadista*", disponibile su: https://www.analyticaintelligenceandsecurity.it/ricerca-e-analisi/terrorismo/i-finanziamenti-del-terrorismo-jihadista/

[30] Beccaro A. (2018), "ISIS: storia segreta della milizia islamica più potente e pericolosa del mondo", Newton Compton editori s.r.l., Roma.

[31] Napoleoni L. (2014), "ISIS, lo stato del terrore: l'attacco all'Europa e la nuova strategia del califfato", Feltrinelli Editore Milano.

della banca. Queste ultime applicano l'imposta sui conti bancari e deducono dal patrimonio il 2,5%, per poi versare la somma ad organizzazioni filantropiche islamiche.
Altri fondi, che hanno un ruolo non trascurabile per il finanziamento del terrorismo, provengono dalle Organizzazioni Non Governative e dalle Organizzazioni senza scopo di lucro islamiche. Spesso si tratta di associazioni pseudo caritatevoli, che raccolgono i finanziamenti, per alimentare le azioni dei gruppi terroristici. Queste organizzazioni, per gestire i capitali, si servono di canali formali, mentre nel momento in cui devono trasferire le somme raccolte ai gruppi terroristici, si avvalgono di mezzi informali, quali l'hawala[32], strumento frequentemente usato nel mondo islamico e di cui si approfondirà la natura e il funzionamento nei paragrafi successivi.

2.2.2 Differenza tra sistemi formali e sistemi informali

Al fine di comprendere perché il sistema islamico dell'*hawala* possa costituire una minaccia, è necessario analizzare la differenza tra i canali formali e quelli informali di trasferimento di denaro.
Vengono definiti canali formali tutti quei sistemi che consentono di trasferire denaro e che si servono di operatori o strumenti regolati dalla legge e sottoposti al controllo di un'autorità.
L'utilizzo di canali formali prevede lo svolgimento di specifiche procedure, che hanno la finalità di provare e tenere traccia dell'avvenuto trasferimento di denaro. Infatti, è prevista la stipula di un contratto, formalmente intestato, nel quale vengono determinati i diritti e i doveri del cliente e dell'intermediario.
Al contrario, si definiscono canali informali, quei sistemi che non si avvalgono di operatori e non sono controllati da alcuna autorità. L'informalità del sistema ha sia risvolti positivi, in termini di costo e di facilità di utilizzo, che risvolti negativi, primo fra tutti, la rischiosità. A differenza dei canali formali, le operazioni informali di trasferimento del denaro sono svolte senza autorizzazioni e controlli e soprattutto senza la stipula di un contratto. Non sono richieste formalità come, per esempio, la richiesta di documenti, che identifichino le parti coinvolte, fattore che rende il processo più semplice, ma anche molto rischioso. Non essendo perfezionato un contratto che sancisca l'accordo, le parti coinvolte non possiedono alcuna tutela legale. Poiché l'accordo è concluso verbalmente, si basa esclusivamente sul rapporto di fiducia tra i contraenti.[33]

[32] Ibidem

[33] Cit. *Hawala e Finanza. Le vie segrete del denaro nell'era dell'economia globale,* Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali – CSSII.

2.3 La bipolarità dell'*hawala*

Il finanziamento delle attività organizzative ed operative del terrorismo necessita di costanti fondi che, come descritto in precedenza, nonostante la finalità illecita, è possibile provengano da fonti lecite. Il trasferimento dei fondi può avvenire attraverso dei meccanismi informali che ne rendono difficile l'individuazione; uno degli strumenti più diffusi nel mondo islamico è l'*hawala*.
L'importanza ricoperta da questo sistema di finanziamento di attività terroristiche è stato compreso solo dopo gli attentati dell'11 settembre 2001. La Commissione d'Inchiesta che ha redatto il *9/11 Commission Report,* ha rintracciato la provenienza dei fondi utilizzati da Al-Qaeda e ha identificato le procedure con cui l'organizzazione gestisce i fondi. Nel report viene specificato come l'organizzazione terroristica utilizzi un sistema informale per trasferire le proprie risorse, l'*hawala*, sistema privilegiato dai gruppi terroristici, in quanto dotato di tipicità di cui i sistemi bancari tradizionali sono sprovvisti. L'*hawala,* appartenendo alla categoria dei sistemi informali, si adatta alle esigenze delle organizzazioni terroristiche, in quanto sistema "sicuro" in termini di anonimato.
Hawala è un termine che in arabo significa "scambiare" o "trasformare" e si tratta di un sistema molto consolidato nel mondo islamico, in quanto si basa su un rapporto fiduciario tra le parti. Il circuito dell'*hawala* funziona bene in quei paesi in cui è forte il concetto di fiducia, radicato nella cultura islamica e che permette alle persone di affidare i propri soldi senza timore.
Questo canale, diffuso particolarmente in Medio Oriente, Africa ed Asia, è sorto al fine di trasferire fondi legittimi e con fini altrettanto leciti, per far fronte ai rischi legati allo spostamento internazionale del denaro, nonché per colmare la carenza di sistemi bancari in alcune aree del mondo. L'*hawala* però nonostante sia sorta con finalità lecite, si è poi anche diffuso anche come strumento di finanziamento di atti terroristici.[34]

2.3.1 Il funzionamento e le caratteristiche dell'*hawala*

A differenza degli istituti bancari, che operano solo come persone giuridiche e sono circuiti in cui l'esecuzione della transazione è concordata attraverso un contratto i cui attori sono solo il mittente e il destinatario, nel sistema *hawala* partecipano attivamente quattro soggetti.

[34] Rossi A. (2020), Risk compliance *"Hawala: un sistema (illegale) per il finanziamento al terrorismo"*, disponibile su: https://www.riskcompliance.it/news/hawala-un-sistema-illegale-per-il-finanziamento-al-terrorismo/

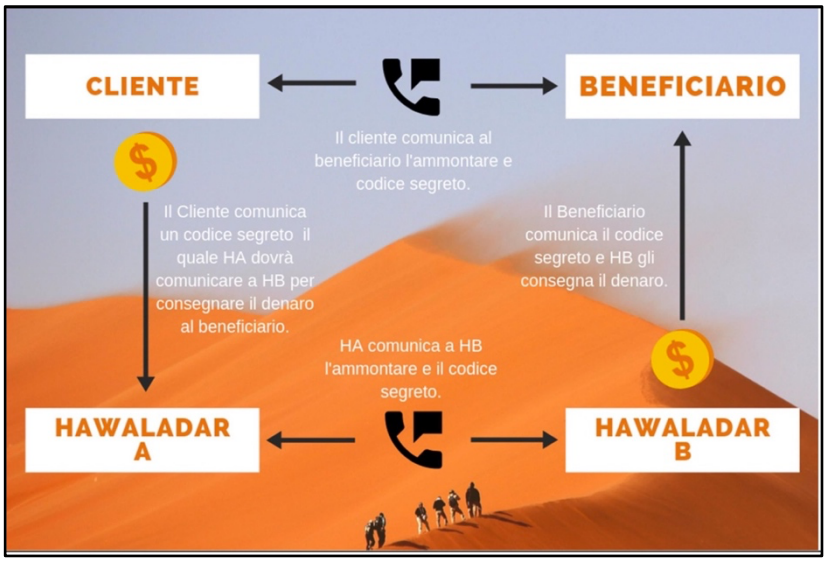

Figura 5- Modello di sintesi (Elaborazione Antonio Rossi)[35]

Nel sistema dell'*hawala* partecipano quattro soggetti: il cliente, colui che intende trasferire il denaro, il beneficiario e due *hawaladar* che svolgono il ruolo di intermediari, uno che si trova nel luogo di partenza del denaro e ha il compito di contattare il secondo intermediario, che si trova nel luogo di destinazione.

Dalla rappresentazione sopra riportata si deduce che il sistema *hawala* segue questo procedimento:

1. Il cliente si rivolge all' *hawaladar A* in quanto desidera trasferire dei fondi al beneficiario, il quale si trova nel paese dove opera l'*hawaladar B*. Quest'ultimo verrà così contattato dall'*hawaladar* che agisce per il cliente: saranno stati inoltre determinate le commissioni della transazione e l'eventuale cambio delle valute del trasferimento, tasso di cambio compreso;
2. Nel momento in cui il cliente consegna i fondi al *hawaladar* A, autorizza la transazione tramite una parola d'ordine, che comunica all'intermediario A e al beneficiario;
3. L'*hawaladar A* comunica poi all'*hawaladar B* i dettagli della transazione e la parola d'ordine, che il beneficiario dovrà imprescindibilmente riferire se desidera accedere ai fondi;
4. Completate le operazioni citate, l'*hawaladar B* può trasferire i fondi al beneficiario;
5. Successivamente i due *hawaladar* si accordano sulle partite di debito/credito, che gestiscono attraverso compensazioni periodiche.

Acquisito lo svolgimento del processo, è opportuno analizzare ora le principali caratteristiche che permettono di identificarlo come un sistema funzionale:

[35] Cfr. https://www.riskcompliance.it/news/hawala-un-sistema-illegale-per-il-finanziamento-al-terrorismo/

- *Velocità di esecuzione*: i trasferimenti sono portati a termine in 24 ore;
- *Convenienza*: l'*hawaladar* richiede delle commissioni basse;
- *Anonimato*: è un sistema esente da adempimenti burocratici, quindi il trasferimento dei fondi viene effettuato basandosi solamente sulla conoscenza reputazionale e sull'onesta del cliente, elementi considerati sufficienti;
- *Affidabilità*: è una caratteristica che si desume dall'elemento principale che ne gestisce il funzionamento, la fiducia;
- *Versatilità*: è un circuito che, grazie alla facilità di implementazione, si presta ad essere utilizzato anche in quei paesi dove sono carenti sistemi finanziari convenzionali.

Il circuito dell'*hawala* è considerato legale nei seguenti paesi: gli Emirati Arabi Uniti, il Pakistan, l'Afghanistan e l'India; è considerato invece un sistema illegale in molti paesi occidentali.
È comunque possibile affermare che nonostante sia ritenuto illegale, è un sistema diffuso in Europa di cui i terroristi si sono serviti per finanziare, ad esempio, gli attentati del 2015 di Parigi.[36]

2.3.2 L'anonimato delle transazioni: l'alleato delle organizzazioni terroristiche

La principale caratteristica del circuito *hawala*, vantaggiosa dal punto di vista dei gruppi terroristici, è la possibilità di trasferire denaro senza che alcuno spostamento fisico dello stesso. Il sistema si basa su trasferimenti che avvengono per via telefonica e sono gestiti tramite sistemi di compensazione. Il circuito dell'hawala, inoltre, garantisce l'anonimato, in quanto, come già visto, non sono previsti documenti che testimonino l'esistenza di un accordo tra i clienti. Gli *hawaladar* tengono dei registri, che non sono accessibili a soggetti terzi, in quanto si tratta di documenti personali, su cui gli intermediari segnano le transazioni a cui hanno preso parte. Le annotazioni degli *hawaladar* sono utili agli stessi solo al fine di tenere traccia delle movimentazioni e soprattutto delle somme da ricevere e da saldare.
In questo sistema informale non esiste un contratto con valore legale, ma ci sono solo documenti personali utili a controllare le transazioni effettuate nel corso del tempo; caratteristica, che impedisce alle autorità esterne di controllare qualsiasi documentazione.
È, quindi, possibile concludere che proprio la caratteristica dell'informalità e dell'anonimato rendono tale canale quasi invisibile, un ottimo alleato per il finanziamento occulto delle organizzazioni terroristiche.

[36] Cit. Risk compliance *"Hawala: un sistema (illegale) per il finanziamento al terrorismo.*

CAPITOLO 3 – CYBER JIHAD E FINANZA 2.0

Operando un'analisi delle modalità di finanziamento delle organizzazioni terroristiche, è interessante approfondire nello specifico il legame con le nuove tecnologie. Il terrorismo sfrutta a proprio vantaggio le innovazioni tecnologiche, sia per diffondere l'ideologia estremista con attività di propaganda, sia in ambito finanziario come canale di finanziamento. Tale modalità operativa ha permesso alle organizzazioni terroristiche di potenziare velocità ed efficienza comunicativa.
Analizziamo quindi le modalità con cui i gruppi terroristici si servono di internet e quali sono i canali privilegiati per implementare la propaganda, per comprendere poi le operazioni più innovative che vedono coinvolto il mondo del fintech e le criptovalute.

3.1 Cyber jihad: la comunicazione del califfato

Il ricercatore dell'università di Oxford, Aymenn Jawad al-Tamimi, che ha studiato le azioni del Califfo Abu Bakr al-Baghdadi dal 2011, afferma quanto segue: *"Si serve del web per diffondere in maniera sofisticata e professionale l'invito alla jihad adoperando non solo i siti estremisti tradizionali ma anche i social network, e riuscendo a trasformare la sua ideologia in un contagio".*
Il livello di preparazione raggiunto dalla jihad digitale si è compreso nel 2015 a seguito dell'attacco degli hacker del "cyber-Califfato", contro il Comando centrale Usa a Tampa.
L'idea di agire anche sul piano digitale fu sviluppata da Osama bin Laden, leader di al-Qaeda, che comprendendo l'influenza della tecnologia, scrisse una lettera ai suoi sostenitori per sottolineare l'importanza di questo strumento. Abu Hamza al-Muhajir, uno dei leader di "al-Qaeda in Iraq", colse tale richiesta e, come affermato nell'ordine dell'aprile 2010, iniziò a chiedere alle cellule di reclutare "*chi dimostra interesse per gli hacker, al fine di distruggere i siti Internet del nemico e infiltrare le sue roccaforti strategiche"*, convinto del fatto che *"la guerra elettronica è uno strumento della guerra del futuro"* [37]. Quando lo stesso anno Abu Bakr al-Baghdadi subentra al comando di "al-Qaeda in Iraq", sembra voler seguire la stessa linea del predecessore, ritenendo che la realtà digitale rappresenti una via attraverso la quale è possibile espandere il Califfato. Egli, infatti, incaricò il Media Center di ricercare jihadisti con elevate capacità informatiche.
Il "cyber-Califfato" è oggi in grado di agire grazie all'operato di Abu Hussain al-Britani, nato a Birmingham, volontario in Siria, nonché impegnato nelle operazioni digitali dell'Isis e ucciso nell'agosto 2015.

[37] Cit. *"Il califfato del terrore: perché lo stato islamico minaccia l'occidente"*, RCS Libri Editore S.p.A., Milano.

È stato colui che ha dato vita al gruppo di jihadisti cibernetici, capaci di sviluppare il software criptato che permette di operare e comunicare tramite social network ed app resistendo ad attacchi informatici[38].

Prima di analizzare come il terrorismo utilizzi il web, di seguito viene riportata una tabella che permette di comprendere come, nonostante la strategia mediatica sia variegata, ogni strumento implementato abbia una finalità specifica e la più importante sia il raggiungimento di un impatto pervasivo.

Tipologia (e prodotti)	*Target*	*Obiettivo*	*Strategia*	*Medium preferito*
Social Media (FB, twitter, ecc.)	Potenziali sostenitori, radicali islamisti, ecc.	Radicalizzazione, reclutamento	Promuovere comportamenti virali e imitativi; *story telling*	Piatta-forme social
Comunicazione dell'orrore (le decapitazioni)	I nemici del califfato, pubblico occidentale ampio	Terrorizzare e minacciare	Mostrare la brutalità della morte, promuovere reazioni affettive	Video
Contro-informazione (Cantlie: Lend Me Your Ears e reportage)	Pubblico occidentale competente e interessato	Promuovere il dibattito su IS insistendo sui temi critici dell'agenda pubblica occidentale	Realizzare contro narrative: ricontestualizza-zione dei contenuti nella prospettiva di IS	Video
Informazione (Islamic State News e brochure diverse)	Famiglie di (potenziali) sostenitori; pubblico occidentale critico all'intervento contro IS	Normalizzare: diffondere notizie che evidenziano la normalità della quotidianità nel califfato	Realizzare contro narrative: ricontestualizza-zione dei contenuti nella prospettiva di IS; promozione della normalità della vita nel califfato	Pdf
Magazine, Ebook (*Dabiq*, *Inspire*, ecc.)	Membri di IS soprattutto *foreign fighters* ma anche audience occidentale competente	Chiarire e indirizzare sul piano politico, teologico e tattico	Utilizzare un medium "tradizionale" e una pluralità di strategie	Pdf
Gamification (Grand Theft Auto: Salil al-Sawarim)	Giovani digitali, non solo islamisti	Socializzare con il califfato e IS	Utilizzare il gioco come veicolo di socializzazione e normalizzazione	Gioco in rete
Convergenza (KhilafaLive, gamification,…	Distribuzione di tutti i temi già utilizzati dalla comunicazione di IS, rivolgendosi a un pubblico ampio, che troverà "ambiti di nicchia" propri per lingua e orario di programmazione			Web TV

Figura 6 – Sintesi delle strategie comunicative di IS [39]

[38] Ibidem.

[39] Cfr. https://www.ispionline.it/sites/default/files/pubblicazioni/twitter_jihad_comunicazione_isis_0_0.pdf

Le capacità delle organizzazioni terroristiche di sfruttare la tecnologia si sono evolute nel tempo e tale perfezionamento si nota nel diverso utilizzo del web e nelle diverse finalità che i gruppi terroristici gli hanno attribuito. Al-Qaeda, infatti, inizialmente si limitava a postare dei messaggi videoregistrati di Osama bin Laden e video in cui venivano mostrati gli addestramenti. Più di recente, invece, la jihad si è servita di internet per pubblicare dissertazioni sul Corano, per comunicare sui social network, per pubblicare video di alta qualità finalizzati a spiegare non solo come si combatte e chi sono i nemici, ma anche per pubblicizzare lo stile di vita che si conduce sotto la guida dello Stato Islamico.

I jihadisti si servono del web anche per diffondere il messaggio ideologico e un ruolo importante è ricoperto dai c.d. *"disseminatori della jihad"*, soggetti assimilabili ai lupi solitari, ma della realtà digitale, in quanto rientrano nella strategia del Califfo per divulgare l'odio verso gli infedeli e la conoscenza dello Stato Islamico. I forum sviluppati nel tempo sul web hanno la finalità di reclutare soggetti già convinti dell'ideologia per affidargli la divulgazione della stessa, sempre con l'ausilio del web. Quando si parla di disseminatori spesso si fa riferimento a miliziani che sono impegnati al fronte, in Iraq o in Siria, o a jihadisti residenti in Occidente e che volontariamente sono attivi sul web, dove postano immagini o video con la finalità di allargare la visibilità dell'operato dello Stato Islamico. Questo modo di operare può risultare vantaggioso, in quanto l'identificazione di tutte le fonti di propaganda da parte delle forze antiterrorismo diviene molto complicata, ma allo stesso tempo, risulta arduo anche per il Califfo tenere sotto il proprio controllo l'operato sul web di tutti i soggetti[40].

Lo Stato Islamico non è stato il primo ad utilizzare i mezzi telematici con finalità strategiche, ma quello che lo distingue dai gruppi terroristici precedenti è il livello di sofisticazione che ha raggiunto nell'utilizzo dei media. La propaganda attuata dallo Stato Islamico ha la finalità di trasmettere un duplice messaggio. Da un lato, vengono pubblicati video per mostrare atti di violenza, ma allo stesso tempo, viene pubblicizzato lo stile di vita condotto nella comunità dello Stato Islamico.

Per il Califfato la propaganda ha iniziato a ricopre una grande importanza, tale che ha deciso di dotarsi di un Consiglio per i Media. Lo scopo del consiglio è quello di incrementare le adesioni e reclutare volontari attraverso la propaganda sul web. Nello specifico si occupa delle dichiarazioni ufficiali, dell'utilizzo dei social media, di estendere la produzione di materiale propagandistico come canzoni, video, testi e riviste e ha anche il compito di preservare la sicurezza dei siti del Califfato.

La propaganda ha assunto nel tempo sempre più un'importanza globale; infatti, secondo il report 2021 redatto dall'Europol sulla situazione e l'andamento del terrorismo nell'UE, negli ultimi anni i

[40] Cit. *"Il califfato del terrore: perché lo stato islamico minaccia l'occidente"*, RCS Libri Editore S.p.A., Milano.

gruppi jihadisti si sono serviti di app come WhatsApp o Telegram, per inviare messaggi in modo istantaneo e criptato, finalizzati al reclutamento e al coordinamento di eventuali attacchi.
I terroristi sono attivi anche sui social network, quali Facebook e Twitter, utilizzati anch'essi per ingaggiare nuove reclute, usate a loro volta come strumento di propaganda. Si parla in questo caso di *cyber-mujaheddin*, soggetti che riescono a controllare il traffico dei tweet attraverso l'utilizzo di hashtag. Per esempio, The Independent ha evidenziato come i jihadisti abbiamo utilizzato l'evento dei mondiali di calcio del 2014 come mezzo di propaganda, in quanto attraverso hashtag come #Brazil2014, #ENG, #France e #WC2014, rimandavano a contenuti dello Stato Islamico e promuovevano dei video raffiguranti atti violenti.[41]
Per quanto riguarda la produzione dei video, il Califfato si serve di società di produzione come Al-Furqan e Al-Hayat Media Center, le quali permettono di offrire una qualità di definizione elevata. Alla pubblicazione dei video si affianca anche la propaganda attraverso le riviste, tra le quali la più importante è stata "*Dabiq"*, divenuta, nel 2016 *"Rumiyah",* attiva fino a qualche anno fa.
Da questa analisi è quindi possibile dedurre che la propaganda, svolta soprattutto sul web, rappresenta uno dei pilastri su cui si fonda la previsione espansiva dello Stato Islamico.

3.1.1 La radicalizzazione e gli "atti di jihad individuale"

"*La Commissione europea definisce radicalizzazione violenta il fenomeno che vede persone abbracciare opinioni, vedute e idee che potrebbero portare ad atti terroristici*"[42].
La radicalizzazione è sempre più in crescita e non solo nel mondo islamico, in quanto ormai ha assunto portata internazionale. Il fondamentalismo religioso è il principale fattore che caratterizza la radicalizzazione, ma la religione e l'ideologia, da sole, non incrementano questo fenomeno che spesso si manifesta in individui insoddisfatti dalle loro vite, dalla società e dalla politica dei governi. Ciò porta a dire che non è possibile individuare, a priori, i soggetti che teoricamente potrebbero essere interessati ai movimenti estremisti, ma è possibile dedurre che coloro che hanno subito

[41] Cfr. Fifi G. (2017), *"Dall'Avanguardia Rivoluzionaria alla Mobilitazione Intelligente: Come l'ISIS ha Cambiato la Narrativa del Terrorismo",* Il diritto penale della globalizzazione, disponibile su: https://www.dirittopenaleglobalizzazione.it/dallavanguardia-rivoluzionaria-alla-mobilitazione-intelligente-come-lisis-ha-cambiato-la-narrativa-del-terrorismo/

[42] Cfr. Parlamento europeo (2021), *"Cos'è e come si può prevenire la radicalizzazione nell'Unione europea?"*, disponibile su: https://www.europarl.europa.eu/news/it/headlines/security/20210121STO96105/cos-e-e-come-si-puo-prevenire-la-radicalizzazione-nell-unione-europea

discriminazioni o hanno perso la propria identità, potrebbero essere coinvolti nel reclutamento radicalizzante.

Gli attentati terroristici che hanno avuto luogo negli ultimi anni in Europa permettono di comprendere che il fenomeno della radicalizzazione rappresenta ormai da anni un rischio anche per l'UE, in quanto molti degli attacchi sono stati eseguiti proprio da cittadini europei. Questa tendenza sembra essere anche alimentata dallo sviluppo delle nuove tecnologie[43].

I ricettori del messaggio propagandistico sono singoli estremisti o micro-cellule e particolarmente pericoloso è il fenomeno dei Foreign fighters e dei c.d. "lupi solitari".

I Foreign fighters sono una categoria di soggetti reclutati grazie alla propaganda digitale, combattenti stranieri convertiti all'islam radicale e partiti da diversi paesi per combattere in Iraq o in Siria e sostenere le organizzazioni jihadiste[44].

L'utilizzo del web da parte dei jihadisti ha avuto un ruolo importante anche nella nascita dei "lupi solitari", singoli individui che, attraverso l'acquisizione di contenuti e immagini condivise su internet, decidono spontaneamente di abbracciare l'ideologia jihadista e di intraprendere attacchi individuali, non coordinati con altri e che li rendono difficili da individuare e prevenire.

Fu Anwar al-Awlaki, l'imam del New Mexico e poi capo di "al-Qaeda in Yemen", a rivoluzionare la propaganda jihadista. Inizialmente, la comunicazione era caratterizzata solo da lunghi discorsi del leader di al-Qaeda, Osama bin Laden, finalizzati a raggiungere un numero ristretto di spettatori, in quanto erano registrati in lingua araba. Prima di essere ucciso nel 2010, al-Awlaki colse l'inefficienza di questo tipo di comunicazione per reclutare nuovi seguaci dell'ideologia jihadista, decidendo di istituire un nuovo mezzo di comunicazione, la rivista, che prese il nome di "Inspire", si tratta di un magazine, scritto in lingua inglese, la cui finalità era dare inizio ad una "open source jihad", fomentando i lettori attraverso accuse nei confronti dei "nemici dell'islam" e dove era anche possibile trovare istruzioni su come costruire una bomba o come intraprendere attacchi nei confronti degli infedeli[45]. Anwar al-Awlaki può quindi essere considerato il primo leader di al-Qaeda che sia riuscito a raggiungere, attraverso il suo nuovo modo di fare propaganda e con l'ausilio dei social media, quei soggetti che non erano avvicinati dalla comunicazione di Osama bin Laden. Egli fu quindi il primo a

---

[43] Cfr. Parlamento europeo (2021), *"Cos'è e come si può prevenire la radicalizzazione nell'Unione europea?"*, disponibile su: https://www.europarl.europa.eu/news/it/headlines/security/20210121STO96105/cos-e-e-come-si-puo-prevenire-la-radicalizzazione-nell-unione-europea

[44] A cura di Plebani A. (2016), "Jihad e terrorismo, da al-Qaida all'ISIS: storia di un nemico che cambia", ISPI, istituto per gli studi di Politica Internazionale.

[45] Cit. *"Dall'Avanguardia Rivoluzionaria alla Mobilitazione Intelligente: Come l'ISIS ha Cambiato la Narrativa del Terrorismo",* Il diritto penale della globalizzazione.

rivolgersi a quegli individui che oggi sono conosciuti come "lupi solitari". La volontà di Anwar al-Awlaki di accrescere sempre di più il numero di seguaci, deriva da una ideologia secondo la quale: *"piccole cellule, completamente separate le une dalle altre sono in grado di indebolire l'Occidente e risvegliare lo spirito di resistenza dei musulmani grazie ad atti di jihad individuale"*[46].

Questi atti, eseguiti individualmente da soggetti distaccati dalle organizzazioni jihadiste, rappresentano, oltre che una modalità di agire più efficiente per indebolire gli infedeli, anche un modo meno pericoloso in termini di ripercussioni negative per le altre organizzazioni.

La finalità era quella di evitare che si ripetesse ciò che si è verificato dopo l'attentato dell'11 settembre 2001, quando al-Qaeda si è ritrovata a dover affrontare la controffensiva americana in Afghanistan e non solo.

Dal 2016 il Califfato ha iniziato a perdere il controllo di alcuni territori nell'area siro-irachena, fattore che ha portato a un ridimensionamento dell'organizzazione. Nonostante la perdita di aree geografiche, vi è stato un potenziamento della propaganda, soprattutto quella rivolta all'incentivazione di atti di jihad individuale[47]. Anche il 2020 ha rappresentato un anno di riorganizzazione per lo Stato Islamico, dopo l'ulteriore perdita territoriale e la scomparsa, nel 2019, del leader al-Baghdad. Si è osservata una riduzione della propaganda e della capacità di mettere in atto attacchi sofisticati in Occidente, ma dai recenti avvenimenti emerge una nuova strategia. Non è stata manifestata la volontà di ricostruire lo Stato territoriale nella regione siro-irachena, ma l'organizzazione mira ad attuare un assetto decentralizzato e a mantenere centralizzate solo le funzioni di coordinamento e controllo[48].

Sempre nel corso del 2020, a causa delle restrizioni alla circolazione per effetto della pandemia di COVID-19, sono diminuite le possibilità per i jihadisti di effettuare propaganda attraverso incontri fisici, ma è stato osservato un ingente flusso di attività online[49].

Pur non essendo stato rilasciato alcun audio o video dal nuovo califfo, Abu Ibrahim al-Hashimi al-Qurashi, tuttavia i seguaci dello Stato Islamico, che operano online, hanno continuato a sostenere la propaganda, soprattutto quella rivolta ai lupi solitari, affinché intraprendessero attacchi individuali.

---

[46] Cit. *"Il califfato del terrore: perché lo stato islamico minaccia l'occidente"*, RCS Libri Editore S.p.A., Milano.

[47] Relazione sulla politica dell'informazione per la sicurezza - 2017, Roma, Presidenza del Consiglio dei Ministri, Sistema di Informazione per la Sicurezza della Repubblica, 2018. Disponibile su:
https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2018/02/Relazione-2017.pdf

[48] Relazione sulla politica dell'informazione per la sicurezza - 2020, Roma, Presidenza del Consiglio dei Ministri, Sistema di Informazione per la Sicurezza della Repubblica, 2021. Disponibile su:
https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2021/02/RELAZIONE-ANNUALE-2020.pdf

[49] EUROPOL, *"European Union Terrorism Situation and Trend report 2021"*, disponibile su:
https://www.europol.europa.eu/cms/sites/default/files/documents/tesat_2021_0.pdf

Dal 2018 inoltre, l'Europol combatte la lotta al terrorismo online collaborando con Telegram, che nel novembre 2019 ha iniziato a prendere delle misure per rimuovere dalla propria piattaforma i gruppi terroristici. Tale attività, proseguita anche nel 2020, ha reso difficile l'operato dei sostenitori online, obbligati a ingegnarsi per cercare una nuova rete di comunicazione[50].

3.2 Fintech: la tecnologia al servizio del terrorismo

Da quanto sviluppato nei paragrafi precedenti si può comprendere come il jihadismo abbia ormai assunto una diffusione globale, aspetto che ha portato le organizzazioni terroristiche a dover sfruttare le nuove tecnologie anche per velocizzare e aumentare le possibilità di reperire e trasferire denaro.
Sono proprio le innovazioni tecnologiche offerte in ambito finanziario che hanno permesso alle organizzazioni terroristiche di ricorrere a metodi di finanziamento rapidi e anonimi.
La principale minaccia proveniente dal mondo digitale, oltre alla propaganda e alla comunicazione finalizzate al reclutamento, è la raccolta di fondi online, anche mediante l'utilizzo di piattaforme di *crowdfunding*, un metodo finalizzato a raccogliere donazioni da un grande numero di persone, che nel caso del finanziamento al terrorismo, vengono raggiunte tramite i social media.
Da qualche anno, l'interesse dei gruppi terroristici si è spostato anche verso un nuovo metodo di finanziamento che permette di utilizzate la moneta virtuale: la più famosa è il bitcoin, che basandosi sulla tecnologia Blockchain consente di effettuare transazioni in modo anonimo e senza essere sottoposti al controllo di un ente terzo, in quanto si tratta di un sistema decentralizzato. Quest'ultima caratteristica permette a chiunque di accedere alla piattaforma, poiché tale metodo, non essendo collegato al tradizionale sistema bancario, come unici strumenti indispensabili per il suo utilizzo richiede un dispositivo elettronico e la connessione internet. Quindi, il carattere innovativo e la disintermediazione, oltre a renderlo un sistema privo di una regolazione, permettono di raffigurarlo come uno strumento che si presta ad essere utilizzato per fini illeciti[51]. Ed è proprio in questo vuoto regolatorio che si insinua il terrorismo; infatti, lo Stato islamico ha iniziato ad affiancare al tradizionale sistema di finanziamento dell'*hawala,* il fundraising mediante criptovalute[52]. I jihadisti,

[50] Ibidem.

[51] Relazione sulla politica dell'informazione per la sicurezza - 2015, Roma, Presidenza del Consiglio dei Ministri, Sistema di Informazione per la Sicurezza della Repubblica, 2016. Disponibile su: https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2016/03/Relazione-2015.pdf

[52] Bucci L. (2021), *"Follow the money: il mercato delle criptovalute e il terrorismo"*, Osservatorio sul mediterraneo – OSMED, disponibile su: https://www.osmed.it/2021/12/15/follow-the-money-il-mercato-delle-criptovalute-e-il-terrorismo/

quindi, che già nell'hawala possiedono un sistema che permette di trasferire denaro e mantenere l'anonimato, hanno nell'uso delle criptovalute, la possibilità di velocizzare i flussi di moneta, in quanto la piattaforma digitale non è soggetta alle tempistiche del trasferimento fisico.

3.2.1 Moneta virtuale: *ḥarām o ḥalāl ?*

Il finanziamento al terrorismo islamico in criptovalute, osservato dal 2012 ad oggi, non supera il milione di dollari e la spiegazione può essere riscontrata in due motivi, uno di natura economica e uno religioso. Nel mondo musulmano, l'utilizzo di queste monete virtuali potrebbe andare contro quanto prescritto dalla religione ed essere considerato *ḥarām*, termine che in arabo significa proibito e nell'islam rappresenta qualsiasi comportamento o situazione vietati dalla fede islamica, antitetico al termine ḥalāl che, al contrario significa lecito. Questo perché i ricavi generati dalle criptovalute possono essere equiparabili a quelli generati dall'usura, ma anche perché l'utilizzo della criptovaluta viene associato al gioco d'azzardo, pratiche proibite dalla religione islamica. Il secondo motivo invece è rintracciabile nella volatilità attribuita al valore di Bitcoin[53].

L'utilizzo della criptovaluta sta però diventando un mezzo accettato e in linea con i concetti della *shari'a* e si assiste alla comparsa di aziende impiegate nel Financial Technology, che svolgono attività lecite e non collegate a gruppi estremisti. Un esempio è l'azienda OneGram, una startup di Dubai che ha coniato una propria moneta stabilizzandone il valore, avendo legato un'unità di moneta ad almeno 1 grammo d'oro[54].

[53] Ibidem.

[54] Surace V. (2020), Analytica for intelligence and security studies: *"Il ruolo delle criptovalute nel sistema di finanziamento delle organizzazioni terroristiche"*, disponibile su:
https://www.analyticaintelligenceandsecurity.it/ricerca-e-analisi/il-ruolo-delle-criptovalute-nel-sistema-di-finanziamento-alle-organizzazioni-terroristiche/

3.3 Criptovalute: tra finanziamento e propaganda ideologica

Per comprendere perché i gruppi jihadisti abbiamo iniziato a raccogliere fondi richiedendo ai seguaci l'esplicito utilizzo delle criptovalute, è necessario analizzare il contesto su un piano ideologico e non economico[55].

Ormai da qualche anno il jihadismo è entrato in una fase di decentralizzazione che permette di mantenere una coesione che non è più legata all'appartenenza a un territorio, ma all'ideologia. Questo fenomeno sta dando vita a numerosi soggetti che agiscono individualmente e che riescono, agevolati dall'utilizzo del web, a mantenere un collegamento grazie al fondamentalismo ideologico. È proprio in questo contesto che il web ricopre un ruolo fondamentale nelle modalità di finanziamento con l'utilizzo della tecnologia Bitcoin. Ciò che ha attirato i gruppi jihadisti non è solo la possibilità di raccogliere fondi, ma anche l'opportunità di far assumere alle criptovalute un ruolo propagandistico. Infatti, secondo quanto è stato possibile analizzare fino ad oggi, le criptovalute hanno rappresentato un metodo di finanziamento veloce, che, grazie alla sua semplicità, sotto il profilo operativo ne permette un utilizzo da parte di tutti; un mezzo, che consente di incrementare la propaganda e allo stesso tempo di raccogliere fondi, ma soprattutto uno strumento utilizzato per ridicolizzare e sfuggire al sistema bancario occidentale [56].

Le organizzazioni jihadiste hanno iniziato a richiedere donazioni a partire dal 2012 e, a differenza delle campagne di raccolta fondi in cui si utilizzavano i sistemi tradizionali, questo nuovo strumento, permettendo di mantenere l'anonimato dei donatori, consente di rendere esplicita la finalità del fundraising stesso.

I leader delle principali organizzazioni terroristiche, però, non hanno accolto le nuove tecnologie e metodologie operative con lo stesso entusiasmo, sia sotto il profilo ideologico, che operativo, anche se, nell'ottobre 2017 il gruppo al-Qaeda in Siria, riscontrando dei vantaggi nell'utilizzo di questo nuovo sistema, per mezzo della rivista al-Haqiqa (la Verità), iniziò ad esortare i lettori a utilizzare i Bitcoin per effettuare delle donazioni. Era la prima volta che un'organizzazione terroristica di rilevante importanza, incoraggiava l'uso delle criptovalute, fenomeno che sta probabilmente ad

[55] Barone D.M. (2019), *"Criptovalute e jihad: Propaganda, ideologia e comunicazione"*, Ministero della difesa, osservatorio strategico rivista n° 1/2019, disponibile su: https://www.difesa.it/InformazioniDellaDifesa/periodico/Periodico_2019/Documents/Numero1/ID_01_2019_criptovalute_jihad.pdf

[56] Ibidem.

indicare la fine della fase di sperimentazione e l'inizio di quella di consolidamento dell'utilizzo di questo strumento per finanziare la jihad[57].

3.3.1 Jihad e criptovalute

Coinbase, uno dei più importanti cripto-exchanger, in un report del 2021, ha mostrato come il successo delle criptovalute sia stato anche dovuto a una crescita di attività illegali. Le transazioni connesse al finanziamento del terrorismo, nel 2020, rappresentavano meno dello 0,05% del volume illecito, dato che permette comunque di affermare che il finanziamento del terrorismo tramite criptovalute è relativamente ancora basso[58].

Secondo l'analisi svolta dal team Coinbase Special Investigations l'organizzazione che è riuscita a raccogliere la maggior parte dei fondi è Ḥamas, *Ḥaraka al-muqāwama al-islāmiyya*, «Movimento della resistenza islamica». Si tratta di un'organizzazione estremista politico-religiosa palestinese, presente soprattutto nella Striscia di Gaza, fondata nel 1987 da A. Yasin, con l'obiettivo di liberare la Palestina dalla presenza israeliana e costruirvi uno Stato islamico. La quantità di criptovaluta raccolta è di gran lunga superiore rispetto a quella messa insieme dalle altre organizzazioni, perché Ḥamas richiede donazioni in BTC in modo attivo sul proprio sito web e su Telegram.

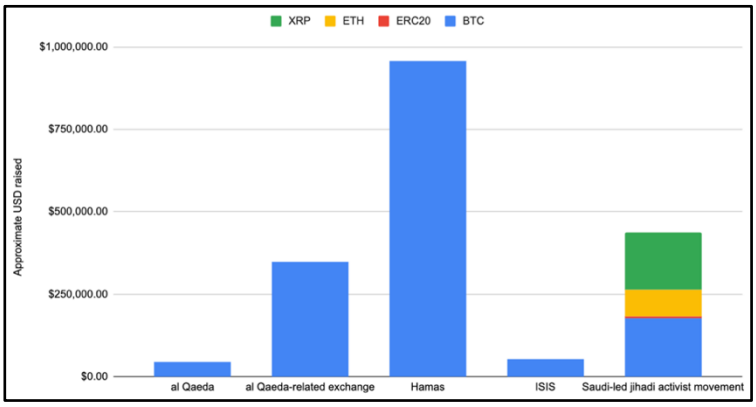

Figura 7 - Raccolta fondi da parte delle organizzazioni più attive legate al TF, per valuta[59]

[57] Ibidem.

[58] The Coinbase Blog (2021), *"Una panoramica dell'uso delle criptovalute nel finanziamento del terrorismo"*. Disponibile su: https://blog.coinbase.com/an-overview-of-the-use-of-cryptocurrencies-in-terrorist-financing-235df6049bc7

[59] Cfr. https://blog.coinbase.com/an-overview-of-the-use-of-cryptocurrencies-in-terrorist-financing-235df6049bc7

Ḥamas ha iniziato a richiedere donazioni in Bitcoin nel 2018, tramite la creazione di un unico indirizzo. Con il tempo, però, al fine di rendere sempre meno tracciabili le transazioni e la quantità dei fondi raccolti, sono stati creati nuovi indirizzi di donazione. Inoltre, come mostra il grafico, la crescente capacità di Ḥamas di raccogliere fondi è visibile soprattutto nei periodi in cui il conflitto assume carattere di maggiore intensità.

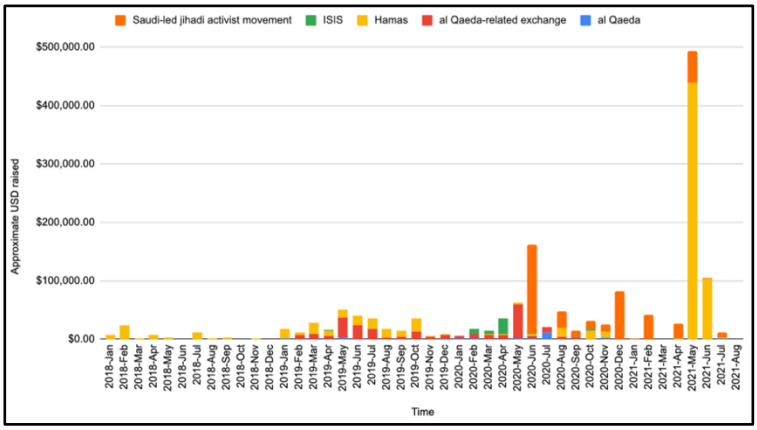

Figura 8 - Raccolta di fondi da parte delle organizzazioni più attive legate al TF, nel tempo[60]

3.3.2 Campagne di raccolta fondi

"*Fund the Islamic Struggle without leaving a trace",* è questo il primo caso di richiesta di utilizzo di criptovalute di cui si ha traccia. Nel 2012 sul deep web fu creata una pagina con lo scopo di promuovere una raccolta fondi tramite i bitcoin. Il sito spiegava i motivi della campagna e chiedeva di contribuire in modo anonimo, ma l'iniziativa fu deludente, in quanto ricevette solo cinque Bitcoin, valore che all'ora corrispondeva a solo 50 dollari[61].

Nel 2014 si rintracciano due casi, uno con finalità economiche e l'altro di natura più ideologica. Nel primo caso fu creato un sito, pubblicato sempre sul deep web e promosso anche su Dabiq, rivista dello Stato Islamico, con la finalità di evidenziare la differenza tra la concezione del gruppo terroristico e il sistema bancario occidentale. L'obiettivo era quello di vendere monete d'oro, d'argento e di rame, ma la novità era la possibilità di utilizzare i bitcoin come mezzo di pagamento e questo per dimostrare la facilità con cui sarebbe stato possibile aggirare il sistema bancario occidentale, che stampa la propria moneta su materiali scadenti.

[60] Cfr. https://blog.coinbase.com/an-overview-of-the-use-of-cryptocurrencies-in-terrorist-financing-235df6049bc7

[61] Azani E., Liv N. (2018), "*Jihadists' Use of Virtual Currency"*. IDC Herzliya – ICT International Institute for Counter-Terrorism, disponibile su: https://www.ict.org.il/images/Jihadists%20Use%20of%20Virtual%20Currency.pdf

Successivamente i jihadisti hanno posto ancora di più l'accento su questo argomento pubblicando un articolo intitolato "*Bitcoin wa Sadaqat al-Jihad"* (Bitcoin e la carità della jihad)[62]. L'articolo, con finalità di propaganda, presenta il sistema Bitcoin come una soluzione per evitare di usare le *"kafir currencies"* (le monete degli infedeli). Si esorta all'uso delle monete virtuali, sia per la loro finalità ideologica e religiosa, sia per le caratteristiche del sistema; infatti, nell'articolo si legge: *"Dark Wallet is a new Bitcoin wallet designed to completely hide the activities of it's users, providing total online anonymity. It eliminates government regulation that tries to identify bitcoins through associating them with an individuals wallets. It mixes all transactions together into an indecipherable mess, making Bitcoin untrackable. This allows our brothers stuck outside of theardh Dawlatul-Islam to avoid government taxes along with secretly fund the mujahideen with no legal danger upon them"*[63].
Da questo estratto si comprende che la volontà del gruppo jihadista era principalmente quella di trasmettere un messaggio, cioè la possibilità di aiutare i mujahideen che si trovano fuori dal territorio dello Stato Islamico a non essere vittime degli articolati sistemi bancari occidentali.
Il primo caso di fundraising connesso a un'organizzazione terroristica è ravvisabile nella campagna di donazioni denominata "*Jahezona"*, che fu messa in atto dall'Ibn Taymiyya Media Center (ITMC), un'unità di propaganda jihadista online e sezione media del Mujahideen Shura Council, un'unione di gruppi salafiti-jihadisti, che operano nella striscia di Gaza. La campagna online di ITMC Jahezona ("Equip us" in arabo) ebbe inizio nel luglio 2015 e chiedeva donazioni per il procacciamento di armi e munizioni, al fine di adempiere all'obbligo di combattere per l'Islam. L'anno seguente e precisamente nel giugno 2016, fu aggiunta la possibilità di fare donazioni anche in bitcoin tramite la pubblicazione su Twitter di QR code che si ricollegavano a un indirizzo bitcoin. La campagna riuscì ad accumulare solo 0,929 BTC, cifra che equivale a circa $540.
Nonostante diverse fonti avessero reso pubblica la campagna di raccolta fondi e i social media iniziassero a limitare l'utilizzo degli account sospetti, ITMC proseguiva nel richiedere donazioni in bitcoin. L'account Jahezona fu eliminato diverse volte da Twitter, ma l'organizzazione continuò ad affidarsi ai suoi seguaci che ritwittavano i contenuti[64].
Nel 2018 la campagna risultò ancora attiva, in quanto, tramite l'account Telegram, l'organizzazione riuscì a pubblicare un nuovo indirizzo bitcoin, che risultò aver ricevuto ben 15 transazioni tra il 2016 e il 2018.

---

[62] Cit. *"Criptovalute e jihad: Propaganda, ideologia e comunicazione"*, Ministero della difesa, osservatorio strategico rivista n° 1/2019.

[63] "*Bitcoin wa Sadaqat al-Jihad"* (2014), disponibile su: https://krypt3ia.files.wordpress.com/2014/07/btcedit-21.pdf

[64] The Chiper Brief (2016), *"The new frontier in terror fundraising: Bitcoin",* disponibile su: https://www.thecipherbrief.com/column/private-sector/the-new-frontier-in-terror-fundraising-bitcoin

Fu con questa campagna di raccolta fondi che le organizzazioni terroristiche cambiarono le modalità di richiedere donazioni pubbliche, in quanto le richieste di denaro per finanziare l'operato dei jihadisti potevano ora essere rese esplicite. Non c'era bisogno di mascherare gli scopi delle raccolte fondi, ma grazie all'anonimato garantito dalle criptovalute, era possibile manifestare la necessità di fondi per acquistare armi[65].

Un'altra campagna di fundraising fu lanciata online nel novembre 2017, un mese dopo la caduta della capitale dello Stato Islamico, Raqqa. Sul sito Akhbar al-Muslimin (Notizie musulmane), l'organizzazione iniziò a richiedere donazioni in bitcoin per cercare di riavviare l'attività di propaganda. La campagna non ebbe successo perché il sito fu rimosso dall'organizzazione stessa, o bloccato dalle autorità.

In questo stesso periodo, fu lanciata un'altra campagna di donazioni jihadista da parte dell'organizzazione Al Sadaqah (carità in arabo). Si tratta di un gruppo che, attivo sui canali Telegram e Twitter, richiede in modo esplicito donazioni per finanziare la battaglia dei mujahideen contro il regime di Assad in Siria. L'organizzazione pubblicò un post in cui lamentava la scarsità di cibo e di munizioni, ma lo sforzo fu vano, perché ha ricevuto un totale di donazioni che non superano i $1000[66].

Il primo caso documentato di un impiego sofisticato della tecnologia si ha nel 2019, quando Izz ad-Din al-Qassam Brigades (IQB), l'ala militare dell'organizzazione terroristica palestinese Ḥamas, nel gennaio 2019, ha iniziato a richiedere donazioni in bitcoin, riuscendo ad accumulare decine di migliaia di dollari. Le modalità utilizzate sono molto simili a quelle descritte in precedenza, in quanto, anche in questo caso, la richiesta è stata effettuata sul loro sito internet, sul quale hanno pubblicato un QR code che permetteva di visualizzare l'indirizzo bitcoin su cui effettuare le donazioni. Con questo metodo sono riusciti ad ottenere circa $2,000.00[67]. L'organizzazione ha dovuto però cambiare il modus operandi, in quanto le autorità erano riuscite a bloccare l'indirizzo e, per non essere rintracciata di nuovo, decise di utilizzare un portafogli integrato, che aveva la particolarità di creare un indirizzo bitcoin per ogni donatore. Questi ultimi avevano la possibilità di scegliere due modi per effettuare le donazioni: il primo metodo permetteva di utilizzare il sistema dell'hawala; quindi, il donatore doveva solamente consegnare all'hawaladar l'indirizzo bitcoin e la somma in denaro, che poi avrebbe convertito in bitcoin. Il secondo sistema invece permetteva ai donatori di agire con il proprio portafoglio virtuale, che riuscivano a creare grazie alle istruzioni che venivano fornite loro.

---

[65] Cit. *"Criptovalute e jihad: Propaganda, ideologia e comunicazione"*

[66] Ibidem.

[67] Cit. Analytica for intelligence and security studies: *"Il ruolo delle criptovalute nel sistema di finanziamento delle organizzazioni terroristiche.*

Procedendo con questo sistema, a un anno di distanza, nel gennaio 2020, l'ammontare raccolto raggiunse i $10,000.00[68].

L'analisi svolta pone in luce come, nel tempo, le organizzazioni jihadiste hanno iniziato a stimolare le donazioni in bitcoin e come nonostante la tendenza sia in aumento, fino ad oggi i risultati non sono stati eclatanti. L'utilizzo delle criptovalute è utile tra gli attivisti, per supportare gruppi minoritari e soprattutto come strumento di propaganda. Si tratta di un fenomeno che pur essendo più evidente, in quanto le organizzazioni rendono esplicite le finalità terroristiche delle raccolte fondi, risulta ancora più difficile da rintracciare per le autorità, a causa delle caratteristiche della tecnologia Bitcoin, che facilita i jihadisti nel rendere il loro operato ancora più opaco.

***

Era il 1982 quando, a Castelgandolfo, Giovanni Falcone illustrò una nuova tecnica investigativa, fondata sul principio *"Segui i soldi e troverai la mafia"*[69].

Alla luce dell'analisi svolta nel presente elaborato, possiamo ben immaginare quanto possa risultare complessa l'applicazione di tale principio in una realtà globalizzata, in cui il Fintech favorisce scambi finanziari, monetari e commerciali in un'ottica di scarsa tracciabilità. Questo fenomeno va a facilitare l'azione non solo delle mafie, oggetto dell'attenzione di Falcone, ma anche delle organizzazioni terroristiche e di tutti quei decisori occulti in grado, potenzialmente, di destabilizzare le democrazie e gli equilibri geopolitici.

Bitcoin, Hawala, Zakāt, ma anche traffici di stupefacenti e di migranti, insieme ad altre attività illecite finalizzate al finanziamento di soggetti ed organizzazioni devianti, sono e saranno oggetto dell'attenzione degli apparati di sicurezza dei Paesi democratici e delle Alleanze che avranno come obiettivo principale il mantenimento dell'ordine mondiale e la stabilizzazione delle democrazie; compito, questo, reso ancora più arduo da attività – anch'esse finanziate con modalità non facilmente rintracciabili – di disinformazione e controinformazione, da sempre presenti in ogni strategia ideologica, tattica e prospettica.

---

[68] Ibidem.

[69] Galullo R., Mincuzzi A. (2022), *"Segui i soldi, troverai la mafia: un podcast racconta come il «metodo Falcone» fa scuola"*, Il Sole 24 ore, disponibile su: https://www.ilsole24ore.com/art/segui-soldi-troverai-mafia-podcast-racconta-come-metodo-falcone-fa-scuola-mondo-AEezZbZB

Bibliografia

A cura di Plebani A. (2016), *"Jihad e terrorismo, da al-Qaida all'ISIS: storia di un nemico che cambia"*, ISPI - Istituto per gli Studi di Politica Internazionale. Mondadori Editore

Azani E., Liv N. (2018), "*Jihadists' Use of Virtual Currency"*. IDC Herzliya – ICT International Institute for Counter-Terrorism. Accesso effettuato il 23 maggio 2022, disponibile su: https://www.ict.org.il/images/Jihadists%20Use%20of%20Virtual%20Currency.pdf

Barone D.M. (2019), *"Criptovalute e jihad: Propaganda, ideologia e comunicazione"*, Ministero della difesa, osservatorio strategico rivista n° 1/2019. Accesso effettuato il 15 maggio 2022, disponibile su: https://www.difesa.it/InformazioniDellaDifesa/periodico/Periodico_2019/Documents/Numero1/ID_01_2019_criptovalute_jihad.pdf

Beccaro A. (2018), "ISIS: storia segreta della milizia islamica più potente e pericolosa del mondo", Newton Compton editori s.r.l., Roma.

Bitcoin.org. Accesso effettuato il 22 marzo 2022, disponibile su: https://bitcoin.org/it/faq#generale

"*Bitcoin wa Sadaqat al-Jihad"*(2014). Accesso effettuato il 23 maggio 2022, disponibile su: https://krypt3ia.files.wordpress.com/2014/07/btcedit-21.pdf

Blockchain.com, grafici Blockchain. Accesso effettuato il 31 maggio 2022, disponibile su: https://www.blockchain.com/charts

Bucci L. (2021), *"Follow the money: il mercato delle criptovalute e il terrorismo"*, Osservatorio sul mediterraneo – OSMED. Accesso effettuato il 17 maggio 2022, disponibile su: https://www.osmed.it/2021/12/15/follow-the-money-il-mercato-delle-criptovalute-e-il-terrorismo/

Cavicchioli M. (2021), The cryptonomist: *"La storia di Bitcoin dalla nascita ad oggi"*. Accesso effettuato il 20 marzo 2022, disponibile su: https://cryptonomist.ch/2021/05/09/storia-bitcoin/

Dai W. (1998), *B-Money*. Accesso effettuato il 12 marzo 2022, disponibile su: http://www.weidai.com/bmoney.txt

Enciclopedia Treccani, *"jihadismo"*. Accesso effettuato il 23 aprile 2022, disponibile su: https://www.treccani.it/enciclopedia/jihadismo/

EUROPOL, *"European Union Terrorism Situation and Trend report 2021"*. Accesso effettuato il 11 maggio 2022, disponibile su: https://www.europol.europa.eu/cms/sites/default/files/documents/tesat_2021_0.pdf

Fifi G. (2017), *"Dall'Avanguardia Rivoluzionaria alla Mobilitazione Intelligente: Come l'ISIS ha Cambiato la Narrativa del Terrorismo",* Il diritto penale della globalizzazione. Accesso effettuato il 9 maggio 2022, disponibile su: https://www.dirittopenaleglobalizzazione.it/dallavanguardia-rivoluzionaria-alla-mobilitazione-intelligente-come-lisis-ha-cambiato-la-narrativa-del-terrorismo/

Fontana F. (2020), Rivista italiana dell'antiriciclaggio "*Criptovalute e rischi di riciclaggio"*. Accesso effettuato il 13 marzo 2022, disponibile su: https://www.antiriciclaggiocompliance.it/app/uploads/2020/08/Fontana.pdf

Galullo R., Mincuzzi A. (2022), *"Segui i soldi, troverai la mafia: un podcast racconta come il «metodo Falcone» fa scuola"*, Il Sole 24 ore. Accesso effettuato il 2 giugno 2022, disponibile su: https://www.ilsole24ore.com/art/segui-soldi-troverai-mafia-podcast-racconta-come-metodo-falcone-fa-scuola-mondo-AEezZbZB

Garavaglia R. (2018), "*Tutto su Blockchain: capire la tecnologia e le nuove opportunità*", Ulrico Hoepli Editore S.p.A., Milano.

Garofalo D. (2020), Analytica for intelligence and security studies: "*Il finanziamento del terrorismo jihadista*". Accesso effettuato il 23 aprile 2022, disponibile su: https://www.analyticaintelligenceandsecurity.it/ricerca-e-analisi/terrorismo/i-finanziamenti-del-terrorismo-jihadista/

Hughes E. (1993), *"Cypherpunk's Manifesto"*. Accesso effettuato il 12 marzo 2022, disponibile su: https://www.activism.net/cypherpunk/manifesto.html

Maggioni M., Magri P. (2015), "*Twitter e jihad: la comunicazione dell'Isis",* ISPI. Accesso effettuato il 9 maggio 2022, disponibile su: https://www.ispionline.it/sites/default/files/pubblicazioni/twitter_jihad_comunicazione_isis_0_0.pdf

Molinari M. (2015), *"Il califfato del terrore: perché lo stato islamico minaccia l'occidente",* RCS Libri Editore S.p.A., Milano.

Molinari M. (2015), *"Jihad: guerra all'occidente"*, RCS Libri Editore S.p.A., Milano.

Nakamoto S. (2008), *"Bitcoin: un sistema di moneta elettronica peer-to-peer"*. Accesso effettuato il 21 marzo 2022, disponibile su: https://bitcoin.org/files/bitcoin-paper/bitcoin_it.pdf
Nakamoto S. (2008), *"Bitcoin P2P e-cash paper"*. Accesso effettuato il 21 marzo 2022, disponibile su: https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html

Napoleoni L. (2014), "ISIS, lo stato del terrore: l'attacco all'Europa e la nuova strategia del califfato", Feltrinelli Editore Milano.

Palumbo G. (2011), *Hawala e Finanza. Le vie segrete del denaro nell'era dell'economia globale,* Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali – CSSII. Accesso effettuato il 30 aprile 2022, disponibile su: https://www.cssii.unifi.it/upload/sub/hawala-e-finanza-islamica-cssii.pdf

Parlamento europeo (2021), *"Cos'è e come si può prevenire la radicalizzazione nell'Unione europea?"*. Accesso effettuato il 23 aprile 2022, disponibile su: https://www.europarl.europa.eu/news/it/headlines/security/20210121STO96105/cos-e-e-come-si-puo-prevenire-la-radicalizzazione-nell-unione-europea

Passarelli N. (2016), *"Bitcoin e antiriciclaggio"*. Accesso effettuato il 20 marzo 2022, disponibile su: https://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/bitcoin-e-antiriciclaggio.html

Relazione sulla politica dell'informazione per la sicurezza - 2015, Roma, Presidenza del Consiglio dei Ministri, Sistema di Informazione per la Sicurezza della Repubblica, 2016. Accesso effettuato il 23 aprile 2022, disponibile su: https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2016/03/Relazione-2015.pdf

Relazione sulla politica dell'informazione per la sicurezza - 2017, Roma, Presidenza del Consiglio dei Ministri, Sistema di Informazione per la Sicurezza della Repubblica, 2018. Accesso effettuato il 23 aprile 2022, disponibile su: https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2018/02/Relazione-2017.pdf

Relazione sulla politica dell'informazione per la sicurezza - 2020, Roma, Presidenza del Consiglio dei Ministri, Sistema di Informazione per la Sicurezza della Repubblica, 2021. Accesso effettuato il 23 aprile 2022, disponibile su: https://www.sicurezzanazionale.gov.it/sisr.nsf/wpcontent/uploads/2021/02/RELAZIONE-ANNUALE-2020.pdf

Rossi A. (2020), Risk compliance *"Hawala: un sistema (illegale) per il finanziamento al terrorismo"*. Accesso effettuato il 30 aprile 2022, disponibile su: https://www.riskcompliance.it/news/hawala-un-sistema-illegale-per-il-finanziamento-al-terrorismo/

Roy O. (2017), "Generazione ISIS: chi sono i giovani che scelgono il califfato e perché combattono l'occidente", Feltrinelli Editore Milano.

Signorelli A.D. (2018), Il tascabile: *"Le origini di Bitcoin"*. Accesso effettuato il 12 marzo 2022, disponibile su: https://www.iltascabile.com/scienze/origini-bitcoin/

Soldavini P. (2021), *"I bitcoin emessi sono il 90% del totale, il 20% è sparito per sempre"*, Il sole 24 ore. Accesso effettuato il 20 marzo 2022, disponibile su: https://www.ilsole24ore.com/art/i-bitcoin-emessi-sono-90percento-totale-circa-20percento-e-sparito-sempre-AETWwp4

Surace V. (2020), Analytica for intelligence and security studies: *"Il ruolo delle criptovalute nel sistema di finanziamento delle organizzazioni terroristiche"*. Accesso effettuato il 17 maggio 2022, disponibile su: https://www.analyticaintelligenceandsecurity.it/ricerca-e-analisi/il-ruolo-delle-criptovalute-nel-sistema-di-finanziamento-alle-organizzazioni-terroristiche/

The Chiper Brief (2016), *"The new frontier in terror fundraising: Bitcoin",* Accesso effettuato il 23 maggio 2022, disponibile su: https://www.thecipherbrief.com/column/private-sector/the-new-frontier-in-terror-fundraising-bitcoin

The Coinbase Blog (2021), *"Una panoramica dell'uso delle criptovalute nel finanziamento del terrorismo"*. Accesso effettuato il 19 maggio 2022, disponibile su: https://blog.coinbase.com/an-overview-of-the-use-of-cryptocurrencies-in-terrorist-financing-235df6049bc7

Vidino L., Marone F., Entenmann E. (2017), *"Jihadista della porta accanto: radicalizzazione e attacchi jihadisti in occidente",* ISPI - Istituto per gli Studi di Politica Internazionale.
Accesso effettuato il 23 aprile 2022, disponibile su: https://www.ispionline.it/sites/default/files/pubblicazioni/report_jihadista_della_porta_accanto.pdf