

# L'ORIZZONTE DEGLI EVENTI

Quaderni geopolitici e analisi giuridiche

N. 13 - LUGLIO 2023

BITCOIN E CRIPTOVALUTE:  
LIMITI E POTENZIALITÀ

GIANLUCA AURELIO  
GIORGIO CARDILE

ISSN 2724-2315



# ABSTRACT

In 2008, Satoshi Nakamoto published his whitepaper "Bitcoin: A Peer-to-Peer Electronic Cash System" where he describes, in nine pages, how his invention works. The software code, released in 2009, sparked Bitcoin adoption and continuous improvement by its community, as well as the ability to be copied by third parties to create different cryptocurrencies, given its open-source nature.

Bitcoin is a decentralized cryptocurrency that uses a technology called blockchain, a distributed public ledger that records all transactions made permanently and securely. Bitcoin's blockchain ensures the security, incensurability and transparency of transactions, eliminating the need for centralized intermediaries such as banks.

The interest in this technology and its adoption has increased year by year and has seen its expansion into different sectors and for different purposes. Although Bitcoin and cryptocurrencies in the common imagination are often associated with criminal activities, e.g., buying drugs, weapons, paying ransoms to hacker groups, money laundering, or speculative activities, such as trading, in several countries around the world this technology (especially Bitcoin) is showing its true potential by being applied to support human rights, creating circular economies, and improving the energy grid of some countries.

# INDICE

AMISTADES.....	1
L'ORIZZONTE DEGLI EVENTI.....	2
INTRODUZIONE.....	3
1. UTILIZZO NON VIRTUOSO. IL RICORSO AL BITCOIN E ALLE CRIPTOVALUTE PER EVADERE LE SANZIONI INTERNAZIONALI ....	5
1.1 Corea del Nord.....	13
1.2 Russia.....	16
2. UTILIZZO VIRTUOSO.....	21
2.1 El Salvador.....	22
2.2 Guatemala e Costa Rica.....	25
2.3 USA – Texas.....	27
2.4 Africa.....	29
CONCLUSIONI.....	32
BIBLIOGRAFIA E SITOGRAFIA.....	34
HANNO COLLABORATO A QUESTO NUMERO.....	35

# AMISTADES

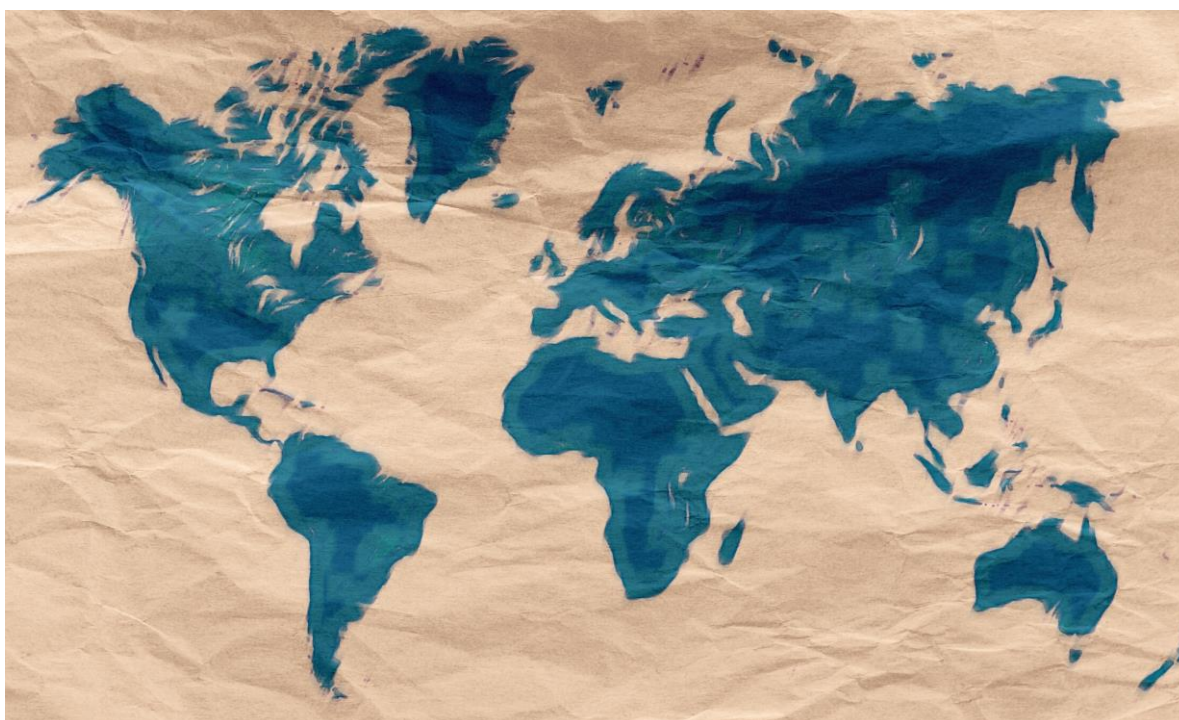


AMISTADES - Fai Amicizia con il Sapere è un Centro Studi indipendente fondato nel 2017 a Roma e impegnato nella diffusione della cultura internazionale.

Il centro si occupa di ricerca, divulgazione e formazione sulle tematiche internazionali, con un particolare focus sulla geopolitica e il diritto internazionale.

Eroga corsi di formazione per istituti scolastici, studenti, professionisti e aziende; realizza analisi geopolitiche e report; organizza eventi e conferenze istituzionali e incontri informali di avvicinamento alle materie trattate.

Al momento di questa pubblicazione, fanno parte di AMISTADES oltre 50 giovani professionisti tra board direttivo e analisti. Tutti animati dalla stessa sete di conoscenza e condivisione.



# L'ORIZZONTE DEGLI EVENTI

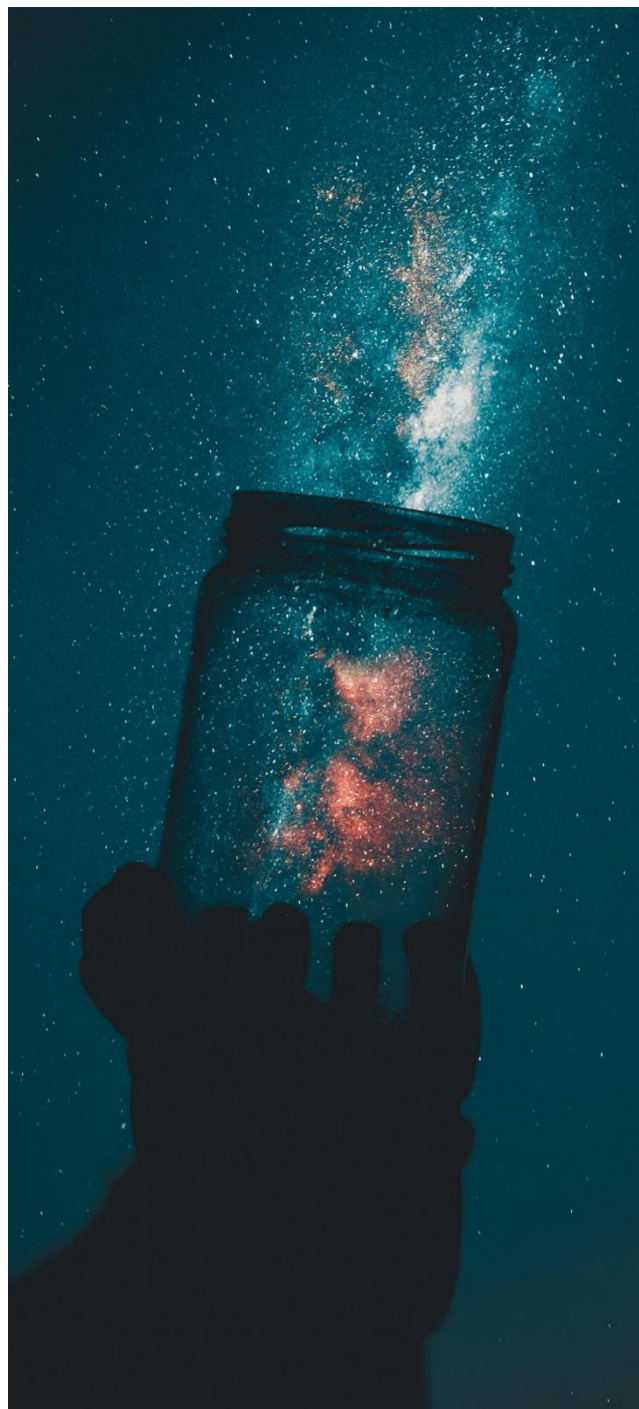
L'Orizzonte degli Eventi è la linea in cui tutto si crea e tutto si distrugge.

Un punto, in astronomia, dal quale non si può più tornare indietro. Una linea immaginaria di confine fra l'universo conosciuto e la forza attrattiva di un buco nero.

È questa la nostra idea di divulgazione. Andare oltre il sapere e conoscere quello che esiste al di là di qualsiasi confine.

E una volta lì, chi vorrebbe tornare indietro?

Così trattiamo tematiche di geopolitica e diritto internazionale, restando fedeli a questo concetto assoluto e inarrivabile. Con il desiderio di spingerci oltre ogni volta, raccontando quello che era, quello che è e quello che potrebbe accadere, scrutando e mettendo ordine in quel buco nero magnetico e caotico che è la realtà.



# INTRODUZIONE

di Gianluca Aurelio e Giorgio Cardile

Nel 2008, Satoshi Nakamoto pubblica il whitepaper "*Bitcoin: A Peer-to-Peer Electronic Cash System*" dove descrive, in nove pagine, il funzionamento della sua invenzione. Bitcoin è un sistema di denaro elettronico puramente *peer-to-peer* che permette l'invio di pagamenti direttamente da un'entità ad un'altra, senza la necessità di una terza parte, ad esempio un istituto finanziario. Il codice del software, rilasciato nel 2009, ha dato il via all'utilizzo e al continuo miglioramento di Bitcoin da parte della community, oltre alla possibilità di essere copiato da terzi per creare differenti criptovalute, data la sua natura open-source. Ma come funziona Bitcoin? Bitcoin è una criptovaluta decentralizzata che utilizza una tecnologia chiamata blockchain. La blockchain di Bitcoin è un registro pubblico distribuito che registra tutte le transazioni effettuate in modo permanente e sicuro. Funziona come un grande registro digitale condiviso tra i nodi che compongono la rete, i quali verificano e validano le transazioni. Ogni blocco contiene un certo numero di transazioni e viene collegato al precedente attraverso algoritmi crittografici, creando una

catena di blocchi immutabile. La blockchain di Bitcoin garantisce la sicurezza, l'incensurabilità e la trasparenza<sup>1</sup> delle transazioni, eliminando la necessità di intermediari centralizzati come le banche. Inoltre, il protocollo Bitcoin si basa sul meccanismo di consenso chiamato *Proof of work* (PoW, prova di lavoro): alcuni partecipanti, i *miner*, attraverso il processo chiamato *mining*, utilizzano degli hardware specifici per risolvere complessi problemi matematici per creare nuovi blocchi e validare così le transazioni effettuate dagli utenti della rete. Chi "scopre" un nuovo blocco viene ricompensato con nuovi Bitcoin al fine di ripagare la potenza di calcolo e l'energia utilizzata dalle macchine.

A differenza di Bitcoin, molte delle principali criptovalute utilizzano un differente meccanismo di consenso, chiamato *Proof of Stake* (PoS). Nella PoS, invece di risolvere problemi computazionali, i partecipanti devono dimostrare la loro "quota" di criptovaluta posseduta e congelata nel sistema. Più criptovaluta si possiede, maggiore è la probabilità di essere scelti per convalidare le transazioni e ricevere

---

<sup>1</sup> Essendo la blockchain un registro aperto e distribuito, per trasparenza si intende il fatto che ogni transazione di bitcoin effettuata è pubblicamente consultabile con un qualsiasi blockchain explorer (es.

<https://mempool.space>). Essendo un mezzo di pagamento pseudonimo il mittente e il destinatario, invece, sono trasparenti ma non direttamente collegati ad un'identità.

ricompense. La PoS richiede meno risorse energetiche rispetto alla PoW. Al tempo stesso, la PoS presenta diversi aspetti negativi: la concentrazione della ricchezza si sposta su pochi utenti, che detengono il maggior numero di criptovalute o token<sup>2</sup>, abbassando così il livello di decentralizzazione e distribuzione della rete e rendendola più vulnerabile ad attacchi del 51%<sup>3</sup>. Inoltre, basandosi sulla quantità di criptovaluta posseduta, disincentiva una partecipazione attiva da parte degli utenti, in quanto richiede un maggiore investimento economico, provocando una minore sicurezza complessiva della rete.

L'interesse nei confronti di questo nuovo mondo e l'adozione di questa tecnologia è aumentato di anno in anno ed ha visto la sua espansione in diversi settori e per diversi scopi, talvolta virtuosi, talvolta criminali. Nonostante Bitcoin e le criptovalute nell'immaginario comune siano spesso associate ad attività criminali, ad esempio acquisto di sostanze stupefacenti, armi, pagamento dei riscatti a gruppi hacker, money laundering, o ad attività speculative, come il trading, in diversi paesi del mondo questa tecnologia (specialmente Bitcoin) sta dimostrando il suo vero potenziale venendo applicata a supporto dei diritti umani, creando economie circolari e migliorando la rete energetica di alcuni paesi.

---

<sup>2</sup> A differenza delle criptovalute che nascono da una loro propria blockchain (es. Bitcoin), i token si appoggiano ad una blockchain esistente (es. Ethereum) e tutte le regole sono gestite tramite *smart contract*.

<sup>3</sup> Un attacco del 51% è un tipo di attacco informatico che si verifica quando un attaccante o un gruppo di attaccanti controlla oltre il 50% del potere computazionale o del potere decisionale all'interno della rete. Ottenuta questa maggioranza, l'attaccante può

manipolare le transazioni e il consenso della rete in vari modi. Ad esempio, potrebbe annullare transazioni confermate, impedire la conferma di nuove transazioni o persino riscrivere la cronologia delle transazioni precedenti.

È importante notare che è altamente improbabile che avvenga un attacco del 51% in Bitcoin, in quanto richiede una quantità significativa di risorse finanziarie e computazionali per acquisire una tale maggioranza.

# 1. UTILIZZO NON VIRTUOSO. IL RICORSO AL BITCOIN E ALLE CRIPTOVALUTE PER EVADERE LE SANZIONI INTERNAZIONALI

di Giorgio Cardile

Prima di poter parlare di come le criptovalute vengono (o possono essere) utilizzate per evadere le sanzioni internazionali, è importante chiarire i criteri metodologici, interpretativi, dare le definizioni e l'obiettivo della ricerca.

'Evadere' una sanzione significa violare una norma creata da uno Stato o da un ente sovranazionale che stabilisce dei divieti nei rapporti economico-commerciali con un determinato Paese, con alcuni suoi enti o organi, con alcune aziende private o con alcune persone fisiche individuate.

Come nel costrutto *if/then* dell'informatica, in queste norme, al verificarsi di determinate condizioni, c'è un risultato. È possibile anche prevedere delle norme che seguono la struttura *if/then/else*, dove *else* indica l'alternativa possibile (o la conseguenza ulteriore) al verificarsi di condizioni diverse.

Chiarito cosa intendiamo per *evadere* e per *sanzione*, passiamo ad *internazionale*.

Se uno Stato è il massimo sovrano di se stesso (*superiorem non recognoscens*), in che modo questo concetto di sovranità si concilia con la possibilità che uno Stato venga sanzionato (subendo un danno economico)?

Secondo l'art. 41 della Carta delle Nazioni Unite, Capitolo VII, rubricato "Azione nei confronti delle minacce alla pace, delle violazioni della pace e degli atti di aggressione" si afferma che "Il Consiglio di Sicurezza può decidere quali misure non implicanti l'uso della forza armata debbano essere impiegate per rendere effettive le sue decisioni e può chiedere ai membri delle Nazioni Unite di applicare tali misure. Queste possono includere l'interruzione totale o parziale delle relazioni economiche e dei mezzi di comunicazione ferroviari, marittimi, aerei, postali, telegrafici, radiofonici e di altro tipo, nonché la rottura delle relazioni diplomatiche".

Facciamo un esempio.



Nel 2017, con la Risoluzione n. 2371, il Consiglio di sicurezza ONU ha inflitto delle sanzioni alla Corea del Nord. Le sanzioni hanno riguardato un divieto di esportazione di ferro, frutti di mare e piombo. Hanno anche incluso il congelamento dei beni esteri della Banca per il Commercio Estero della Corea del Nord.

Non era la prima volta che il Consiglio di sicurezza aveva inflitto sanzioni alla Corea del Nord. L'aveva fatto con la risoluzione 825 (1993), la risoluzione 1540 (2004), la risoluzione 1695 (2006), la risoluzione 1718 (2006), la risoluzione 1874 (2009), la risoluzione 1887 (2009), la risoluzione 2087 (2013), la risoluzione 2094 (2013), la risoluzione 2270 (2016), la risoluzione 2321 (2016) e la risoluzione 2356 (2017), tra le altre.

Le sanzioni possono anche essere rivolte a determinati organi o enti di uno stato, come ministeri, uffici, società pubbliche o istituti di credito statali, fino ad aziende private o a persone fisiche.

Quindi, è possibile che alcuni enti sovraordinati al singolo Paese (nel caso delle risoluzioni del Consiglio di sicurezza, l'ONU), per ragioni inerenti alla tutela della pace globale, concordino su delle norme che modificano la posizione di un singolo Paese.

Anche l'Unione Europea ha irrogato delle sanzioni, e lo fa utilizzando i suoi strumenti normativi, ossia regolamenti e direttive. Ad esempio, importare acciaio dalla Russia è vietato per i paesi europei, ai sensi dell'art. 3g del Regolamento n. 428 del 15 marzo 2022.

Tramite il portale EU Sanctions map<sup>4</sup>, è possibile vedere a quali sanzioni è soggetto quale Paese attraverso una mappa interattiva. Per fare un esempio del contenuto e della portata di questo strumento da parte dell'UE, è possibile consultare l'infografica esplicativa resa dalla Commissione europea per riassumere le sanzioni irrogate alla Federazione Russa.<sup>5</sup>

È anche possibile che un singolo Paese irroghi delle sanzioni. Un esempio tipico di ciò sono gli Stati Uniti, le cui entità sanzionate sono pubblicamente consultabili nel portale dell'Office of Foreign Assets (OFAC)<sup>6</sup>. Le sanzioni possono riguardare il commercio di determinati beni o servizi, know-how, esclusione dall'uso di determinati strumenti finanziari, interruzione delle relazioni diplomatiche o di accordi specifici.

Serve quindi un modo per evadere le sanzioni riducendo questi rischi al minimo. È possibile argomentare che un modo per violare queste norme sia effettuando lo scambio (che è solo uno degli step necessari) pagando con criptovalute.

Esistono degli studi che puntano a misurare il livello di corruzione in un determinato Paese o rispetto a determinati mezzi o attività.

Ad esempio, il Corruption Perception Index (CPI), uno studio rilasciato annualmente dall'ONG Transparency International, prova a farlo con la seguente metodologia.

Secondo la loro documentazione tecnica metodologica allegata all'index del 2022, il

---

<sup>4</sup> consultabile qui: [EU Sanctions Map](#) (ultimo accesso 9 luglio 2023)

<sup>5</sup> consultabile qui: [EU sanctions against Russia over Ukraine \(since 2014\) - Consilium](#) (ultimo accesso 9 luglio 2023)

<sup>6</sup> consultabile qui: [OFAC](#) (ultimo accesso 9 luglio 2023)

CPI si basa su 13 fonti di dati che raccolgono la valutazione di esperti e dirigenti aziendali su una serie di comportamenti corrotti nel settore pubblico, tra cui:

- corruzione;
- diversione di fondi pubblici;
- utilizzo di cariche pubbliche per guadagni privati;
- nepotismo nel servizio pubblico;
- *state capture* (termine coniato dalla World Bank. Secondo il libro "Anticorruption in Transition: Contribution to the Policy Debate" pubblicato dalla World Bank nel 2000, si definisce un ente regolatore statale come 'catturato' quando l'ente regola le aziende in base agli interessi privati (i regolati), invece di perseguire l'interesse pubblico per cui l'ente è stato istituito. Sebbene la *state capture* possa verificarsi attraverso la fornitura di guadagni, sia diretti che indiretti, da parte delle aziende regolamentate ai funzionari statali, non si limita all'influenza attraverso tentativi di corruzione)<sup>7</sup>;

Alcune fonti esaminano anche i meccanismi disponibili per prevenire la corruzione in un Paese, come ad esempio:

- la capacità del governo di far rispettare i meccanismi di integrità;
- l'efficace perseguimento dei funzionari corrotti;

- la 'burocrazia', da intendersi come la lunghezza e la complicatezza delle procedure e dei procedimenti amministrativi (ad esempio, il numero e il tipo di documenti da produrre, il contenuto richiesto, gli enti coinvolti nella decisione, il loro grado di discrezionalità, i termini entro cui il procedimento deve proseguire e concludersi, il livello di standardizzazione, digitalizzazione e automazione);
- l'esistenza di leggi adeguate sulla divulgazione finanziaria, sulla prevenzione dei conflitti di interesse e sull'accesso alle informazioni;
- la protezione legale per gli informatori, i giornalisti e gli investigatori (in parte, ciò che intendiamo per whistleblowing, ma anche la libertà di stampa e la trasparenza).

La metodologia include tra i criteri di affidabilità metodologica e reputazione istituzionale l'allineamento concettuale dei dati, comparabilità dei dati tra Paesi e la disponibilità di dati pluriennali.

Successivamente, si procede alla standardizzazione dei dati. Quest'ultima converte tutti i punti assegnati durante la valutazione in una scala da 0 a 100, dove 0 rappresenta il livello più alto di corruzione percepita e 100 il livello più basso di corruzione percepita. La maggior parte delle

---

<sup>7</sup> World Bank (2000). Anticorruption in Transition: Contribution to the Policy Debate. World Bank Publications. ISBN 9780821348024, p. 3 "The definition of state capture used in this report is derived from the concept of regulatory capture, already well established in the economics literature." State regulatory agencies are said to be "captured" when they regulate businesses

*in accordance with the private interests of the regulated as opposed to the public interest for which they were established. Though regulatory capture can occur through the provision of private gains, both direct and indirect, by regulated businesses to state officials, it is not limited to influence through corrupt means."*

fonti da cui trae i suoi valori il CPI computano i punteggi con gli stessi criteri (punteggi più bassi corrispondono a livelli più elevati di corruzione percepita). Altre tre fonti vengono scalate al contrario (punteggi più alti corrispondono a livelli più alti di corruzione percepita).

Le fonti vengono poi invertite moltiplicando ogni punteggio per -1. Dopo, per creare dei modelli statistici validi per i Paesi per cui i dati sono minori o mancanti, viene utilizzato un software per il calcolo statistico chiamato Stata (il comando inserito è *'impute'*).

Si procede poi con un'aggregazione dei dati e un calcolo del margine di incertezza (quest'ultimo punto è stato inserito a seguito di una raccomandazione contenuta in un audit del European Commission Joint Research Centre sulla coerenza concettuale e statistica del CPI, la formula per il calcolo degli errori standard è stata modificata a partire dalla versione del 2018).

Seguono poi altri step.

È stato fornito questo primo approccio alle tecniche metodologiche di studi così colossali per dare un'idea di quanto sia complesso calcolare quanto e come avviene un fenomeno umano che per sua natura si muove nell'ombra.

Chiarito quanto è complesso e limitato il calcolo della corruzione in un determinato Paese con modelli statisticamente rilevanti, passiamo a come si può calcolare rispetto al mercato delle criptovalute.

Esistono studi mirati anche su questo, in particolare sono stati consultati il Crypto Crime Report del 2023 (preparato annualmente dall'azienda americana Chainalysis, che analizza la blockchain –

dove vengono registrate tutte le transazioni – che è pubblicamente accessibile e tracciabile) e il White paper di Satoshi Nakamoto, pseudonimo del creatore del Bitcoin (la cui vera identità è ignota).

Partiamo dal contestualizzare il valore dell'evasione tramite crypto rispetto a quanto si stima sia l'evasione globale. Più o meno questo valore viene collocato tra il 2 e il 5% del Pil globale (800 miliardi – 2000 miliardi di dollari).

Secondo i dati del report del 2023, gli indirizzi illegali (ossia soggetti a sanzioni internazionali o legati a soggetti sanzionati) hanno inviato criptovalute per un valore di 23,8 miliardi di dollari nel 2022. Le attività illegali rappresentano, quindi, solo lo 0,24% del totale dei trasferimenti di criptovalute analizzati. Bisogna precisare che, nel Crypto crime report, le stime sono a ribasso, in quanto si stima esistano conti che operano illegalmente indisturbati. A dimostrazione di ciò, viene fatto presente che i dati sul totale evaso delle edizioni precedenti sono stati rialzati. Nel report del 2021, ad esempio, il valore è stato alzato da 14 a 18 miliardi di dollari. Si tratta di un aumento del 28%.

Passiamo a quanti di questi 23,8 miliardi sono collegabili all'evasione di sanzioni internazionali.

Il 43% del volume di transazioni illecite del 2022 (circa 10 miliardi) proviene da attività associate a entità sanzionate, in un anno in cui l'OFAC ha aggiunto l'exchange Garantex. L'ha fatto nell'aprile 2022, ma in quanto azienda con sede in Russia, Garantex ha potuto continuare ad operare sul mercato. Per le aziende soggette alla giurisdizione degli Stati Uniti, transazioni associate a

Garantex comportano multe e potenziali accuse penali.

È importante chiarire che i fondi ricevuti da Garantex rappresentano gran parte del volume illecito del 2022, secondo la metodologia del report. Anche se la maggior parte di questa attività è probabilmente (secondo lo studio) costituita da utenti russi che utilizzano una borsa russa, la maggior parte dei professionisti della compliance la considera un'attività illecita.

Scendendo più nel dettaglio sulle ragioni della sanzione inflitta ai soggetti che le evadono tramite crypto, segue un grafico estratto da pagina 13 del Crypto Crime Report del 2023.

Name	Reason for sanction
Lazarus Group	Hacking and crypto theft on behalf of North Korean government
Ahmad Khatibi Aghada	Ransomware
Amir Hossein Nikaeen Ravari	Ransomware
Alex Adrianus Martinus Peijnenburg	Drug trafficking
Matthew Simon Grimm	Drug trafficking
Hydra Marketplace	Darknet market and money laundering
Garantex	Money laundering
Blender.io	Money laundering
Tornado Cash	Money laundering
Task Force Rusich	Russian paramilitary group in Ukraine

Tra questi, Hydra era un mercato darknet esteso globalmente fino a quando i suoi server sono stati sequestrati dalla polizia tedesca, contestualmente alla sua designazione come soggetto sanzionato da parte dell'OFAC nell'aprile 2022. Con sede in Russia, Hydra facilitava la vendita di droghe e offriva anche servizi di riciclaggio di denaro.

Tornado Cash, invece, è un servizio di mixing decentralizzato (ossia fa molte microtransazioni tra vari conti per rendere difficile tracciare da quale conto è stato autorizzato un pagamento. Attenzione: è un servizio che può anche essere utilizzato in maniera completamente legale) sulla blockchain di Ethereum. Sanzionato dall'OFAC ad agosto 2022 (e di nuovo a novembre) per aver facilitato il riciclaggio di denaro, principalmente in relazione ai fondi rubati in attacchi da parte di cybercriminali connessi alla Corea del Nord. Tornado Cash è attualmente l'unico protocollo Decentralized Finance (DeFi). Con DeFi si intende la finanza decentralizzata, ossia quei servizi finanziari disponibili online che non si appoggiano ad intermediari, come le banche, ma operano in autonomia sulla blockchain o usando gli smart contracts<sup>8</sup>.

In quanto protocollo DeFi, non è scontato 'staccare la spina' a Tornado Cash con la

stessa facilità con cui lo si potrebbe fare con un servizio centralizzato (per usare un termine da film d'azione con improbabile attacco hacker, Tornado Cash non ha un 'mainframe' in cui è possibile 'entrare' premendo tantissimi tasti in pochi secondi su un prompt di comandi col testo verde o blu elettrico).

Seguendo l'analisi della blockchain è possibile sapere qualcosa in più su chi svolgeva transazioni con questi servizi, prima che venissero sanzionati.

Nel seguente grafico, è stata definita come transazione illecita un'attività in cui una o più parti sono associate con un'entità (un portafoglio legato a un ente sanzionato in questo caso) che compie illeciti. Si osserva il dato contrario per stimare che un portafoglio operi lecitamente.

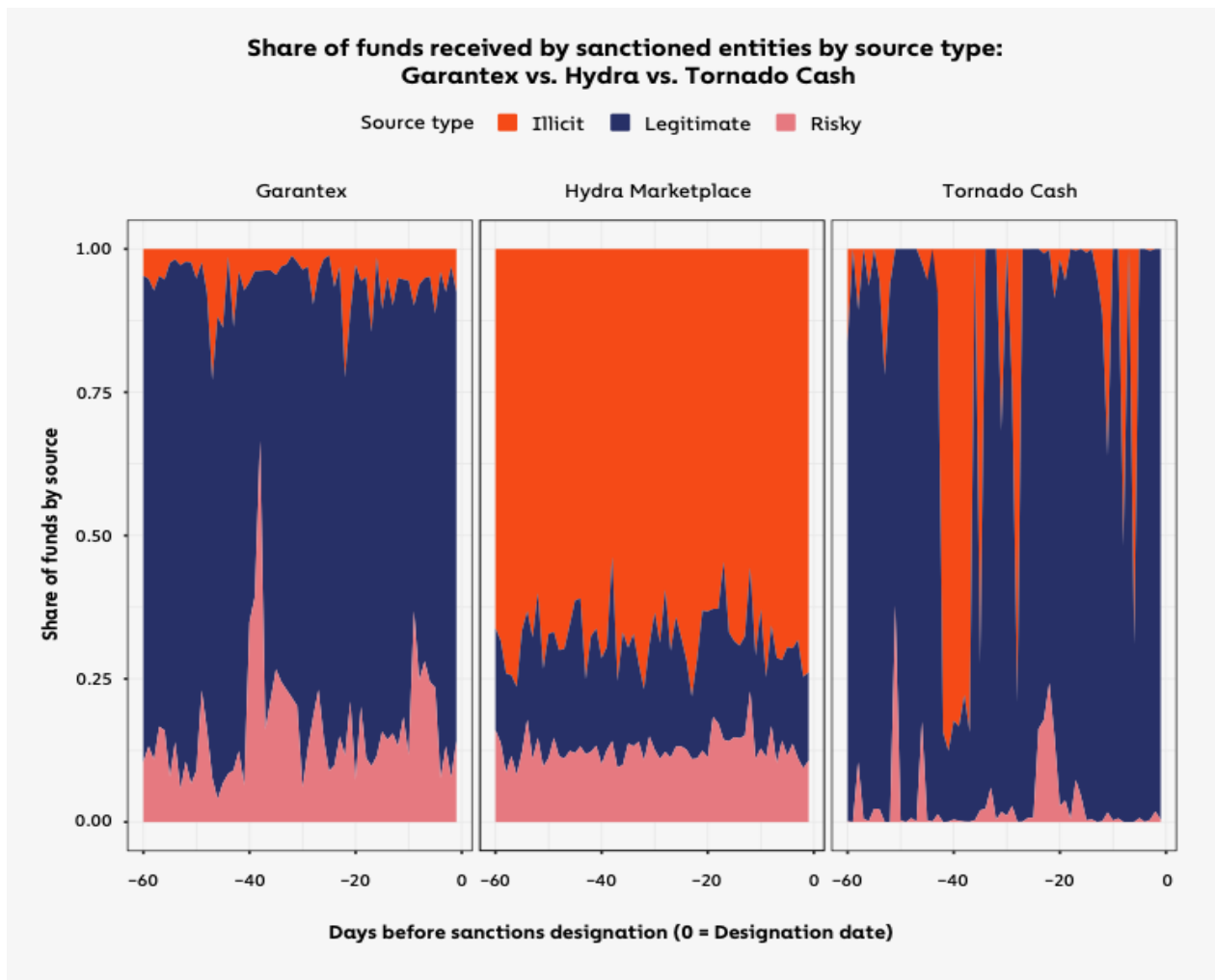
Hydra si classifica primo, con il 68.2% del suo volume proveniente da indirizzi illeciti, e il 12.6% proveniente da indirizzi sospetti.

---

<sup>8</sup> "Smart Contract" è un termine utilizzato per descrivere il codice informatico che esegue automaticamente tutto o parte di un accordo ed è memorizzato su una piattaforma basata su blockchain. [...] Il codice stesso viene replicato su più nodi di una blockchain e, pertanto, beneficia della sicurezza, della permanenza e dell'immutabilità offerte da una blockchain. Questa replica significa anche che, quando ogni nuovo blocco viene aggiunto alla blockchain, il codice viene, di fatto, eseguito. Se le parti hanno indicato, avviando una transazione, che determinati parametri sono stati soddisfatti, il codice eseguirà la fase innescata da tali parametri. Se non è stata avviata alcuna transazione, il codice non eseguirà alcun passo. La maggior parte dei

contratti intelligenti sono scritti in uno dei linguaggi di programmazione direttamente adatti a tali programmi informatici, [...].

Attualmente, i parametri di ingresso e le fasi di esecuzione di un contratto smart devono essere specifici e oggettivi. In altre parole, se si verifica "x", si esegue la fase "y". Pertanto, i compiti effettivi che i contratti intelligenti svolgono sono piuttosto rudimentali, come ad esempio spostare automaticamente una quantità di criptovaluta dal portafoglio di una parte ad un'altra quando vengono soddisfatti determinati criteri. Tratto da [An Introduction to Smart Contracts and Their Potential and Inherent Limitations](#) (ultimo accesso: 9 luglio 2023)



Garantex 6.1% illeciti e 16.1% sospetti. Questo 16% è il più alto come volume di indirizzi sospetti. È ancora più alto se paragonato al volume totale degli indirizzi sospetti nei mercati centralizzati: 0.3%. Questo potrebbe essere un possibile indicatore per una prevalenza di indirizzi sospetti in exchange DeFi. Potenzialmente, quindi, potrebbe esserci un volume di transazioni illecite non noto negli exchange di questo tipo.

Andando avanti, Tornado conta un 34% di volume proveniente da conti illeciti, ma con dei picchi molto irregolari (come si può

evincere dalle grandi colonne rosse nel grafico più a destra).

A pagina 22, il report fornisce informazioni circa l'efficacia delle sanzioni inflitte. Hanno proprio cercato di rispondere alla domanda "se fossi un cryptocriminale che si affida a uno (o più) di questi servizi di riciclaggio di denaro, ho visto meno entrate del previsto dopo che quel servizio è stato sanzionato?".

Sulla base dei dati analizzati dal report, la categoria più colpita sono stati gli amministratori di cybercriminali<sup>9</sup>. Questi ultimi hanno visto un calo nelle entrate di circa 750mila dollari, per via della chiusura dei

<sup>9</sup> Lo studio intende riferirsi con questo termine a indirizzi che sono stati attribuiti a persone collegate a un'organizzazione criminale informatica, come un mercato darknet. Tratto da: [Russian Cybercriminals Drive](#)

[Significant Ransomware and Cryptocurrency-based Money Laundering Activity - Chainalysis](#) (ultimo accesso 16 luglio 2023)

servizi di riciclaggio del denaro che utilizzavano. L'unica categoria influenzata positivamente dalle sanzioni è stata quella degli shop online che truffano (definiti scam), con 5000 dollari circa di entrate stimate.

Inoltre, questi calcoli mostrano solo la variazione media stimata dei ricavi per gli utilizzatori dei servizi di riciclaggio di denaro sanzionati. Con diversi operatori distinti in ciascuna categoria che avevano precedentemente utilizzato tali servizi di riciclaggio di denaro, le perdite totali stimate per categoria dovrebbero essere più elevate.

C'è un altro dato da tenere in considerazione nell'interpretazione di questi dati. L'impatto delle sanzioni sul mercato crypto varia in base alla giurisdizione e ai limiti dettati dalla tecnologia. Abbiamo già visto come Garantex comportasse delle vere e proprie conseguenze prevalentemente sulle realtà soggette alla giurisdizione americana, potendo continuare ad operare.

Ma si possono fare altri esempi.

In primo luogo, il caso di Hydra (dove l'irrogazione delle sanzioni è avvenuta congiuntamente a un'operazione della polizia tedesca) mostra come le sanzioni possono essere estremamente efficaci contro le entità con operazioni chiave in giurisdizioni cooperative. I server di Hydra si trovavano in Germania e le forze dell'ordine tedesche si sono coordinate con le agenzie statunitensi, muovendosi insieme per sequestrare i server di Hydra, oltre alle sanzioni imposte dall'OFAC sul mercato darknet.

Tornado Cash, per la sua natura DeFi, ha subito uno *shut-down* parziale. I suoi smart contracts possono (tecnicamente) operare indefinitamente. C'è comunque stato un calo

degli incassi del 68% nei 30 giorni successivi alle sanzioni.

Un'ultima considerazione sul calcolo estimativo della corruzione nel mondo.

Si può riflettere sul fatto che i dati possono portare a darci risposte che non ci aspettiamo o che non riteniamo possano provenire da dati corretti. Questo è noto come bias della conferma. È la tendenza a cercare, interpretare, concentrarsi e ricordare le informazioni in un modo che conferma i propri preconcetti (ad esempio, magari in pochi si sorprenderebbero a leggere che il Botswana è ritenuto più corrotto dell'Italia, ma se ci fosse scritto il contrario?). Questo pregiudizio di solito si verifica quando la persona che legge dei dati ha un'ipotesi predeterminata e l'analisi dei dati viene svolta con l'obiettivo di dimostrare che si ha ragione. Eppure, non solo il Botswana, ma anche Qatar, Emirati Arabi, Taiwan, Cile, Bhutan e le Bahamas sono considerate meno corrotte dell'Italia. Quanto è sorprendente questa notizia rispetto a sapere che nei primi tre posti si collocano Danimarca, Finlandia e Nuova Zelanda?

Approfondiamo adesso alcuni aspetti di Paesi soggetti a sanzioni internazionali dove si sono svolte attività come quelle che stiamo analizzando.

## 1.1 Corea del Nord

Questo Paese è sanzionato per molte ragioni, ma è anche coinvolto nelle attività del gruppo Lazarus. Nello specifico, secondo un comunicato stampa del Dipartimento del tesoro degli USA del 2 marzo 2020<sup>10</sup>, l'OFAC designa 田寅寅, Tian Yinyin (Tian), e 李家东, Li Jiadong (Li), per aver materialmente assistito, sponsorizzato o fornito supporto finanziario, materiale o tecnologico, beni o servizi a sostegno di crimini informatici. Tian e Li sono stati designati anche per aver materialmente assistito, sponsorizzato o fornito supporto finanziario, materiale o tecnologico o beni o servizi al Lazarus Group.

È stato ricostruito questo accaduto dal medesimo comunicato. La Repubblica Popolare Democratica di Corea (DPRK) addestra questi soggetti a prendere di mira e riciclare i fondi rubati da istituzioni finanziarie. Come primo step, Tian e Li hanno ricevuto da conti controllati dalla Corea del Nord circa 91 milioni di dollari, rubati durante un attacco di aprile 2018 ad un'exchange. Hanno il compito di ripulire quei soldi.

Nello stesso periodo, un dipendente dell'exchange rapinato nel 2018 scarica involontariamente un malware attribuito al DPRK via mail, che permette ai cybercriminali di accedere da remoto alle informazioni personali dei clienti, come le chiavi private dei portafogli. Vengono rubate chiavi private per un valore di 250 milioni di dollari.

Tian, infine, sposta l'equivalente di circa 34 milioni di dollari di questi fondi illeciti

attraverso un conto bancario aperto di recente e collegato al suo conto di scambio. Ha anche trasferito quasi 1,4 milioni di dollari di Bitcoin in carte regalo Apple iTunes prepagate, che in alcuni exchange possono essere utilizzate per l'acquisto di altri Bitcoin. Come fa? Probabilmente ha usato i mixer. Introdotti prima, i mixer sono un servizio di offuscamento. I mixer funzionano raccogliendo crypto da più utenti, 'mescolandole' insieme e inviando a ciascun utente un importo equivalente a quello versato (facciamo un paragone con le monete: se si mettono 5 euro a moneta in una scatola, ne vengono restituiti altri 5, che però non sono gli stessi di prima. Ogni moneta, probabilmente, proviene da un mucchio diverso). Il risultato è che la criptovaluta di ogni utente può essere rintracciata solo dal miscelatore, piuttosto che dalla sua fonte originale, a meno che non si utilizzino speciali tecniche di analisi della blockchain.

Tian risulta sanzionato dall'OFAC, come si può controllare facilmente tramite il loro portale online.

A seguito delle sanzioni, tutte le proprietà e gli interessi di queste persone negli Stati Uniti o in possesso o controllo di statunitensi (persone fisiche e giuridiche, e per gli stranieri si applica ai loro beni soggetti alla giurisdizione americana) devono essere bloccate e segnalate all'OFAC. Sono anche vietate le transazioni all'interno degli Stati Uniti (comprese quelle solo in transito) che coinvolgano proprietà o interessi di persone sanzionate.

---

<sup>10</sup> consultabile qui: [Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group](#) (ultimo accesso 20 luglio 2023)



## Sanctions List Search

Sanctions List Search is a tool that allows users to search the Specially Designated Nationals and Blocked Persons List ("SDN List") and all other sanctions lists administered by OFAC, including the Foreign Sanctions Evaders List, the Non-SDN Iran Sanctions Act List, the Sectoral Sanctions Identifications List, the List of Foreign Financial Institutions Subject to Correspondent Account or Payable-Through Account Sanctions and the Non-SDN Palestinian Legislative Council List. Given the number of lists that now reside in the Sanctions List Search tool, it is strongly recommended that users pay close attention to the program codes associated with each returned record. These program codes indicate how a true hit on a returned value should be treated. The Sanctions List Search tool uses approximate string matching to identify possible matches between word or character strings as entered into Sanctions List Search, and any name or name component as it appears on the SDN List and/or the various other sanctions lists. Sanctions List Search has a slider-bar that may be used to set a threshold (i.e., a confidence rating) for the closeness of any potential match returned as a result of a user's search. Sanctions List Search will detect certain misspellings or other incorrectly entered text, and will return near, or proximate, matches, based on the confidence rating set by the user via the slider-bar. OFAC does not provide recommendations with regard to the appropriateness of any specific confidence rating. Sanctions List Search is one tool offered to assist users in utilizing the SDN List and/or the various other sanctions lists; use of Sanctions List Search is not a substitute for undertaking appropriate due diligence. The use of Sanctions List Search does not limit any criminal or civil liability for any act undertaken as a result of, or in reliance on, such use.

[Download the SDN List](#)

[Sanctions List Search: Rules for use](#)

[Visit The OFAC Website](#)

[Download the Consolidated Non-SDN List](#)

[Program Code Key](#)

**Lookup**

<b>Type:</b>	All	<b>Address:</b>	<input type="text"/>
<b>Name:</b>	tian yinyin	<b>City:</b>	<input type="text"/>
<b>ID # / Digital Currency Address:</b>	<input type="text"/>	<b>State/Province*:</b>	<input type="text"/>
<b>Program:</b>	All 561-Related BALKANS BALKANS-EO14033	<b>Country:</b>	All
<b>Minimum Name Score:</b>	<input type="range" value="100"/>	<b>List:</b>	All
		<input type="button" value="Search"/> <input type="button" value="Reset"/>	

**Lookup Results: 1 Found**

Name	Address	Type	Program(s)	List	Score
<a href="#">TIAN, Yinyin</a>		Individual	CYBER2; DPRK3	SDN	100

\* U.S. states are abbreviated on the SDN and Non-SDN lists. To search for a specific U.S. state, please use the two letter U.S. Postal Service abbreviation.

SDN List last updated on: 6/29/2023 10:02:42 AM  
Non-SDN List last updated on: 5/19/2023 10:20:51 AM

Viene argomentato che questi fondi rubati vengono poi investiti per mantenere i programmi di sviluppo di armi atomiche della DPRK.

Secondo il paragrafo 141 del Final report of the Panel of Experts submitted pursuant to resolution 2627 del Consiglio di sicurezza ONU del 7 marzo 2023<sup>11</sup>, il Gruppo Lazarus è stato monitorato da una società di cybersecurity mentre distribuiva un rootkit di

Windows (un pacchetto di software dannoso progettato per consentire l'accesso non autorizzato a un pc), sfruttando un exploit in un driver del firmware Dell. Tra gli obiettivi c'era un dipendente di un'azienda aerospaziale. Secondo l'azienda, gli hacker hanno abusato della vulnerabilità CVE-2021-21551<sup>12</sup> che colpisce i driver Dell<sup>13</sup> DBUtil117 utilizzando una backdoor HTTP(S) nota come BLINDINGCAN<sup>14</sup>. Questo malware backdoor

<sup>11</sup> consultabile qui: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N23/037/94/PDF/N2303794.pdf?OpenElement> (ultimo accesso 9 luglio 2023)

<sup>12</sup>Per dettagli sulla vulnerabilità CVE-2021-21551 [www.cvedetails.com/cve/CVE-2021-21551](http://www.cvedetails.com/cve/CVE-2021-21551) (ultimo accesso 9 luglio 2023)

<sup>13</sup>Dell ha fornito aggiornamenti di sicurezza per questa vulnerabilità [DSA-2021-088: Aggiornamento di sicurezza](#)

della piattaforma client Dell per una vulnerabilità di controllo degli accessi insufficiente nel driver dbutil Dell (ultimo accesso 9 luglio 2023)

<sup>14</sup>L'Agenzia per le Infrastrutture e la Sicurezza della Cybersecurity degli Stati Uniti d'America (CISA) ha rilasciato un rapporto di analisi del malware su "BLINDINGCAN". [www.cisa.gov/uscert/ncas/analysis-rapporti/ar20-232a](https://www.cisa.gov/uscert/ncas/analysis-rapporti/ar20-232a) (ultimo accesso 9 luglio 2023)

agisce come un trojan di accesso remoto completamente funzionale che disabilita il monitoraggio della sicurezza sulle macchine compromesse. L'azienda ha inoltre valutato che il Gruppo Lazarus si concentra principalmente su tipi specifici di industrie - aerospaziale e difesa, finanza convenzionale e criptovalute - con l'obiettivo di accedere alle basi di conoscenza interne delle aziende compromesse.

Secondo il Final report of the Panel of Experts submitted pursuant to resolution 2569<sup>15</sup> dell'1 marzo 2023, a pagina 4, *"I cyberattacchi, in particolare sulle attività di criptovaluta, rimangono un'importante fonte di reddito per il Governo della Repubblica Popolare Democratica di Corea"*.

Continua al paragrafo 183, dove afferma che *"secondo un recente rapporto<sup>16</sup> di una società di cybersicurezza, i cyberattori della Repubblica Popolare Democratica di Corea hanno rubato un totale di 400 milioni di dollari di criptovalute nel 2021 attraverso sette intrusioni in borse di criptovalute e società di investimento. Questi attacchi informatici "hanno fatto uso di esche di phishing, exploit di codice, malware e ingegneria sociale avanzata per travasare i fondi dai portafogli 'caldi' connessi a Internet di queste organizzazioni verso indirizzi controllati dalla Repubblica Popolare Democratica di Corea". I fondi di criptovaluta acquisiti dai cyberattori della Repubblica Popolare Democratica di Corea passano attraverso un attento processo di riciclaggio di denaro per essere incassati."*

---

<sup>15</sup> consultabile qui: [S/2022/132](#) (ultimo accesso 9 luglio 2023)

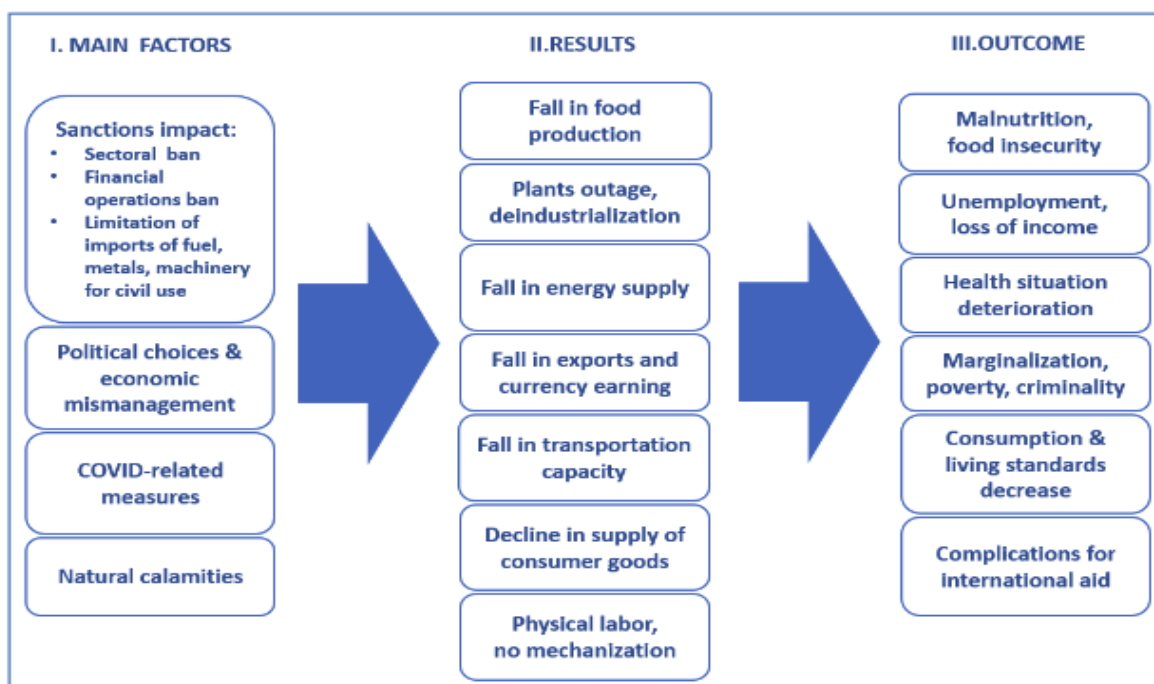
Si stima anche che le sanzioni abbiano anche un impatto non voluto in ambito umanitario. Nello specifico, lo stesso report al paragrafo 188 afferma che *"Tuttavia, ci sono pochi dubbi sul fatto che le sanzioni delle Nazioni Unite abbiano involontariamente influenzato la situazione umanitaria e il diritto allo sviluppo, esacerbando i problemi causati dalla cattiva gestione economica centralizzata e ripiegata su se stessa da parte del Governo della Repubblica Popolare Democratica di Corea. Sebbene l'influenza delle sanzioni non sia il fattore più importante della triste situazione umanitaria, non è stata trascurabile."*

Legano questa affermazione al seguente grafico, presente a pagina 82 del report.

<sup>16</sup> [North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All-time High - Chainalysis](#) (ultimo accesso 9 luglio 2023)

**Figure XLVI**  
**United Nations sanctions as one of several factors causing humanitarian problems (examples)**

*(Factors retrospective since 2018 (after Security Council resolutions), outcomes 2020–2021)*



Source: The Panel.

## 1.2 Russia

Torniamo per un momento al Crypto Crime Report. Abbiamo parlato di Garantex, l'exchange russo sanzionato che copre 10 miliardi di dollari di volume noto di crypto usate per evadere sanzioni internazionali. Si tratta del 43% del totale.

Il grafico di pagina 13 del report del 2023 allegato precedentemente ha come ultimo nella lista la Task force Rusich, un gruppo paramilitare russo che opera in Ucraina, coinvolto anche nella guerra attualmente in corso.

Anche loro sono nell'elenco dell'OFAC, in ragione dell'ordine esecutivo n. 14024 del 15 aprile 2021 del Presidente degli USA, dal titolo *Blocking Property With Respect To Specified Harmful Foreign Activities of the Government of the Russian Federation*. Nel portale è anche possibile vedere gli indirizzi crypto che si ritiene siano legati al gruppo. Secondo il Cambridge Bitcoin Electricity Consumption Index<sup>17</sup> - CBECI (uno studio annuale gestito dal Cambridge Centre for Alternative Finance dell'omonima università inglese) la Russia ha uno share di hash rate<sup>18</sup> mensile di circa il 4.6% (dati di gennaio 2022).

<sup>17</sup> Consultabile qui: [Cambridge Bitcoin Electricity Consumption Index \(CBECI\)](https://www.cambridgecentreforalternativfinance.com/cbeci/) (ultimo accesso 9 luglio 2023)

<sup>18</sup> La definizione di Investopedia è "Il tasso di hash è la misura della potenza computazionale in una rete di criptovalute proof-of-work (PoW). Il tasso di hash viene

utilizzato per determinare la salute, la sicurezza e la difficoltà di mining di una rete blockchain.

Un hash è un codice alfanumerico generato in modo casuale e l'hashing è il processo di indovinare quel codice (o il più vicino possibile). Ogni ipotesi presentata dai computer della rete viene misurata e il tasso di hash è il



## Sanctions List Search

Special Designated Nationals and Blocked Persons list ("SDN List") and all other sanctions lists administered by OFAC, including the Foreign Sanctions Evaders List, the Non-SDN Iran Sanctions Act List, the Sectoral Sanctions Identifications List, the List of Foreign Financial Institutions Subject to Correspondent Account or Payable-Through Account Sanctions and the Non-SDN Palestinian Legislative Council List. Given the number of lists that now reside in the Sanctions List Search tool, it is strongly recommended that users pay close attention to the program codes associated with each returned record. These program codes indicate how a true hit on a returned value should be treated. The Sanctions List Search tool uses approximate string matching to identify possible matches between words or character strings as entered into Sanctions List Search, and any name or name component as it appears on the SDN List and/or the various other sanctions lists. Sanctions List Search has a slider-bar that may be used to set a threshold (i.e., a confidence rating) for the closeness of any potential match returned as a result of a user's search. Sanctions List Search will detect certain misspellings or other incorrectly entered text, and will return near, or proximate, matches, based on the confidence rating set by the user via the slider-bar. OFAC does not provide recommendations with regard to the appropriateness of any specific confidence rating. Sanctions List Search is one tool offered to assist users in utilizing the SDN List and/or the various other sanctions lists; use of Sanctions List Search is not a substitute for undertaking appropriate due diligence. The use of Sanctions List Search does not limit any criminal or civil liability for any act undertaken as a result of, or in reliance on, such use.

[Download the SDN List](#)

[Sanctions List Search: Rules for use](#)

[Visit The OFAC Website](#)

[Download the Consolidated Non-SDN List](#)

[Program Code Key](#)

**Details:**

<b>Type:</b>	Entity	<b>List:</b>	SDN
<b>Entity Name:</b>	TASK FORCE RUSICH	<b>Program:</b>	RUSSIA-EO14024
<b>Remarks:</b>			

**Identifications:**

Type	ID#	Country	Issue Date	Expire Date
Digital Currency Address - XBT	bc1q2lpgjnr348pfvxhfy33ehmdzy3gmxBw4052z26			
Digital Currency Address - ETH	0x3AD9dB589d201A710Ed237c829c7860Ba86510Fc			
Digital Currency Address - ETH	0xc2a3829F459B3Ed87791c74cD45402BA0a20Be3			
Digital Currency Address - USDT	TX5GV4DyfxNB3rPkZzJhmQZ1efVmL4rEqG			
Digital Currency Address - XBT	bc1q7dlyh8xz6tpk92vztrqh88dmjvcwrmsemm			

**Aliases:**

Type	Category	Name
a.k.a.	strong	RUSICH SABOTAGE AND ASSAULT RECONNAISSANCE GROUP
a.k.a.	strong	SABOTAGE AND ASSAULT RECONNAISSANCE GROUP RUSICH
a.k.a.	strong	RUSICH TASK FORCE
a.k.a.	strong	MILITARY-PATRIOTIC CLUB RUSICH
a.k.a.	weak	DSHRG RUSICH

**Addresses:**

Address	City	State/Province	Postal Code	Country
	St. Petersburg			Russia
				Ukraine

[Back](#)

SDN List last updated on: 6/29/2023 10:02:42 AM  
Non-SDN List last updated on: 5/19/2023 10:20:51 AM

Le informazioni usate per ottenere questo dato si basano su un campione esclusivo di dati geolocalizzati delle strutture di mining, raccolti in collaborazione con diverse mining pool<sup>19</sup> di Bitcoin (e secondo i criteri metodologici indicati nella documentazione tecnica dello studio).

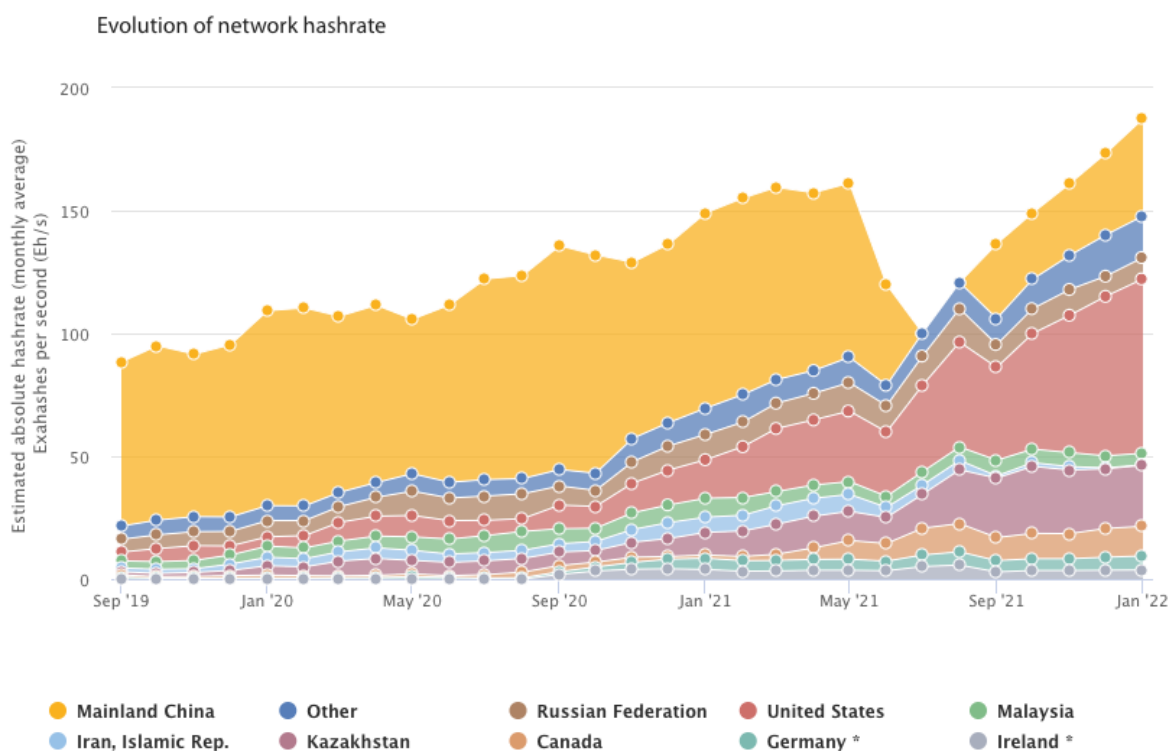
Gli stessi criteri affermano come questi dati potrebbero essere poco rappresentativi in quanto (i) rappresentano meno della metà dell'hash rate totale di Bitcoin e (ii) è dominato da pool di mining precedentemente con sede in Cina.

Anche l'uso di VPN o proxy<sup>20</sup> possono compromettere l'attendibilità di questi dati. Si può determinare una sovrastima (o una sottostima) del tasso di hash rate in alcune province o Paesi. Per un pool di *miners*, questo effetto era particolarmente visibile nella provincia cinese di Zhejiang. Per mitigare questo problema, gli autori dello studio hanno diviso l'hash rate rilevato come proveniente dalla provincia di Zhejiang proporzionalmente tra le altre province cinesi elencate nel set di dati del pool.

numero di ipotesi al secondo che si verificano nell'intera rete." ([Hash Rate](#) - ultimo accesso 16 luglio 2023)

<sup>19</sup> La definizione di Investopedia è "Un pool di mining è un gruppo comune di minatori di criptovalute che combinano le loro risorse computazionali su una rete per rafforzare la probabilità di trovare un blocco o di effettuare con successo il mining di criptovaluta." ([Mining Pool: Definition, How It Works, Methods, and Benefits](#) - ultimo accesso 16 luglio 2023)

<sup>20</sup> Sono meccanismi di connessione sicura tra un dispositivo e una rete. Quando vengono usate, è possibile far credere che ci si stia connettendo da un determinato luogo fisico quando si è in un altro. Questo ha comportato che i dati sulla provenienza dell'hash rate divisi per singolo Paese fossero parzialmente inattendibili.



Questo grafico prodotto dal CBECI mostra il trend dell'hash rate registrato in alcuni Paesi. Inoltre, in Russia, si parla da diversi anni di rublo digitale (definito spesso dai media occidentali cryptorublo).

Il rublo digitale non è una criptovaluta. È una Central bank digital currency<sup>21</sup> (CBDC). Secondo il Consultation paper sul rublo digitale rilasciato dalla Banca di Russia il 13 ottobre 2020, "il rublo digitale è una forma aggiuntiva della valuta nazionale russa che sarà emessa digitalmente dalla Banca di Russia. Il rublo digitale avrà caratteristiche combinate di rubli in contanti e non in contanti.

Come i contanti, sarà possibile utilizzare un rublo digitale offline, ossia senza accesso a

Internet. D'altra parte, la sua forma digitale consente di utilizzare il rublo digitale per i pagamenti online, proprio come i mezzi di pagamento senza contanti.

Tutti gli agenti economici, compresi gli individui, le imprese, i partecipanti ai mercati finanziari e il Governo, avranno accesso al rublo digitale. Tutte e tre le forme del rublo russo saranno assolutamente uguali: come un rublo in contanti equivale a un rublo non in contanti, un rublo digitale sarà sempre uguale a ciascuno di essi."<sup>22</sup>

Il paper poi continua, spiegando perché il rublo digitale non è una criptovaluta.

"Le criptovalute sono totalmente diverse dal denaro delle banche centrali. Le criptovalute non hanno un'unica autorità emittente; non

<sup>21</sup> Si tratta di valute virtuali prodotte e gestite da una banca centrale, nazionale o sovranazionale che sia. La loro caratteristica principale è che ogni pagamento è pienamente tracciabile dall'entità che gestisce il sistema. Viene fornita una sua definizione anche dalla Federal

reserve: [Federal Reserve Board - Central Bank Digital Currency \(CBDC\)](#) (ultimo accesso 9 luglio 2023)

<sup>22</sup> Il Consultation paper è disponibile qui: [https://www.cbr.ru/eng/analytics/d\\_ok/dig\\_ruble/](https://www.cbr.ru/eng/analytics/d_ok/dig_ruble/) (ultimo accesso 9 luglio 2023)

garantiscono la tutela dei diritti dei consumatori; il loro valore è soggetto a una significativa volatilità; è illegale utilizzarle per pagare beni e servizi nella maggior parte dei Paesi<sup>23</sup>; e di solito non hanno un'unica istituzione che ne garantisca la sicurezza. Il rublo digitale è una passività della banca centrale; è implementato attraverso l'uso di tecnologie digitali e non è in alcun modo collegato alle criptovalute. Si tratta di una valuta fiat la cui stabilità è garantita dallo Stato rappresentato dalla banca centrale."

Ancora, nelle Linee guida per l'avanzamento della sicurezza informatica nel settore finanziario per il 2023-2025 pubblicate dalla Banca di Russia il 15 giugno 2023<sup>24</sup>, si menziona ancora il rublo digitale (pp. 13-14, in russo), spiegando che:

- vanno definiti i requisiti di protezione delle informazioni per i partecipanti alla piattaforma di test della CBDC;
- va creato un quadro legale e organizzativo per costruire meccanismi di valutazione della conformità, controllo della resistenza alle minacce attuali e test delle tecnologie applicate, degli algoritmi, degli strumenti tecnici e software in termini di sicurezza delle informazioni;
- devono essere sviluppati meccanismi antifrode (quindi, monitoraggio delle transazioni al fine di identificare le

anomalie che indicano possibili azioni fraudolente), tenendo conto delle specificità delle transazioni di quel tipo.

Continua spiegando come la Banca di Russia "continuerà a creare le condizioni per l'implementazione sicura da parte degli istituti finanziari delle tecnologie digitali e di pagamento attraverso i seguenti progetti:

- sviluppo di nuovi metodi di identificazione e autenticazione;
- lo sviluppo dell'identificazione a distanza per residenti e non residenti;
- lo sviluppo di attività finanziarie digitali, diritti digitali utilizzati e crowdfunding;
- aumento della disponibilità di applicazioni di firma elettronica per il segmento di massa;
- creazione di un operatore del sistema informativo assicurativo automatizzato (AIS), supporto agli uffici di storia assicurativa;
- sviluppo della cooperazione tra gli istituti di credito e finanziari e gli organi esecutivi federali, compreso l'accesso ai sistemi informativi statali (tra cui il Sistema Biometrico Unificato (UBS), il Sistema Unificato di Identificazione e Autenticazione (USIA), GosKluch)."

In un articolo del 2 gennaio 2018 del Financial times<sup>25</sup> viene riportata una dichiarazione di

---

<sup>23</sup> In realtà, diversamente da quanto scritto in questo paper della Banca di Russia, sono pochi i Paesi ad aver dichiarato illegale acquistare, farsi pagare o usare in generale il Bitcoin o altre criptovalute. Per esempio, a pagina 7 e 8 del [PwC Global Crypto Regulation Report 2023 - Amended to include the BCBS rules](#) (ultimo accesso 16 luglio 2023), c'è un elenco dello status legale delle cripto in una serie di Paesi. Solo Qatar, Arabia Saudita e Cina le proibiscono, anche se ci sono altri Paesi

che non hanno ancora un quadro normativo o lo hanno ancora in fase di sviluppo.

<sup>24</sup> Le linee guida sono disponibili qui (in russo): [https://www.cbr.ru/Content/Document/File/148351/onrib\\_2025.pdf](https://www.cbr.ru/Content/Document/File/148351/onrib_2025.pdf) (ultimo accesso 9 luglio 2023)

<sup>25</sup> Reperibile qui (paywalled): <https://www.ft.com/content/54d026d8-e4cc-11e7-97e2-916d4fbac0da> (ultimo accesso 9 luglio 2023)

Sergei Glazev (tra i consiglieri del Presidente della Russia, ex ministro delle relazioni economiche estere sotto Boris Yeltsin, soggetto a sanzioni dall'invasione della Crimea del 2014) che afferma che *“Questo strumento (il rublo digitale, ndr) ci si addice molto bene per le attività sensibili per conto dello Stato. Possiamo regolare i conti con le nostre controparti in tutto il mondo senza tener conto delle sanzioni”*.

## 2. UTILIZZO VIRTUOSO

di Gianluca Aurelio

Bitcoin nasce con l'obiettivo di offrire un'alternativa al sistema finanziario moderno, alle banche centrali. Questa tecnologia è stata creata per superare i limiti e le criticità dell'attuale sistema monetario e proprio grazie alla sua decentralizzazione permette una totale indipendenza dalle autorità governative centrali.

Diversi sono gli esempi dell'applicazione di Bitcoin e del mining a supporto di popolazioni del Terzo Mondo attualmente escluse dal sistema finanziario, dalla possibilità di avere un conto bancario e quindi dotarsi di strumenti fondamentali per la libertà individuale. Dagli ultimi dati raccolti nel 2021 dalla World Bank, sono 1.4 miliardi gli adulti *unbanked*<sup>26</sup>, ovvero che per diversi motivi non hanno accesso ad un conto bancario: mancanza di denaro, distanza elevata da istituti finanziari o documentazione insufficiente. Altrettanti sono i cosiddetti *underbanked*, ovvero persone che hanno un conto bancario, ma alle quali mancano accessi adeguati ai servizi della finanza tradizionale (ad es. l'invio di bonifici, carte di credito, prestiti).

Uno dei primi esempi di utilizzo di Bitcoin a supporto dei diritti umani è stato con il caso

di Julian Assange. A seguito della pubblicazione del materiale sull'era Bush e Obama, WikiLeaks è stata soggetta ad un blocco bancario internazionale: Visa e Mastercard rifiutavano di processare le donazioni e bonifici e PayPal chiuse i conti di Assange e di WikiLeaks. Bitcoin ha trovato terreno fertile per dimostrare una delle sue principali caratteristiche, ovvero l'incensurabilità, oltre alla sua indipendenza dal controllo politico e istituzionale centrale. WikiLeaks, nel 2011, è stata così la prima grande organizzazione ad adottarlo, permettendo a chiunque, da qualsiasi parte del mondo, di inviare pagamenti per sostenere le sue attività e le spese legali.

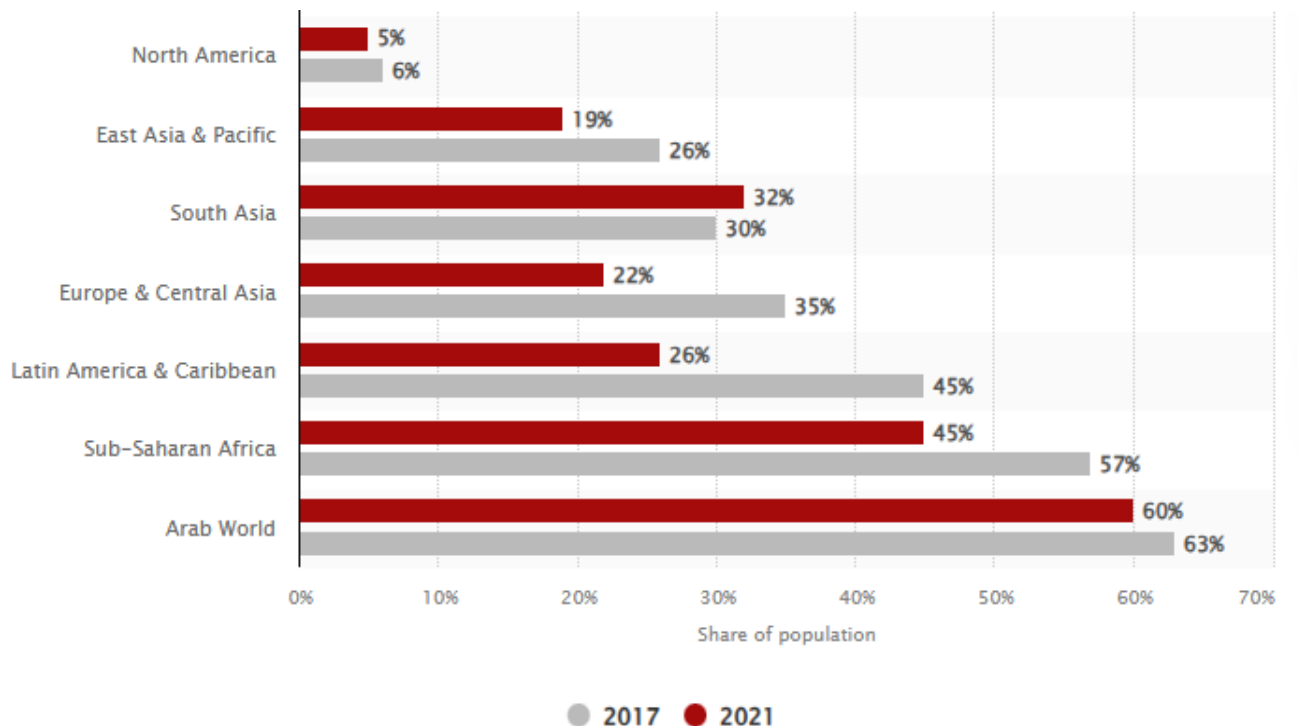
Ma, dal 2011 ad oggi, sono stati fatti diversi passi avanti nell'adozione di Bitcoin in tutto il mondo. Dall'America centrale, al Texas fino all'Africa, verranno presentati alcuni dei principali casi d'uso che questa tecnologia ha trovato.

---

<sup>26</sup>

<https://www.worldbank.org/en/publication/globalindex/interactive-executive-summary-visualization>





## 2.1 El Salvador

Il governo salvadoregno, il 9 giugno 2021, pubblica nella gazzetta ufficiale una legge che vedrebbe Bitcoin come legal tender nel paese. Tre mesi dopo, il 7 settembre 2021, la “Bitcoin Law” diventa effettiva. El Salvador diventa il primo paese ad accettare Bitcoin come valuta a corso legale, affiancando il dollaro. Il governo, guidato da Nayib Bukele, lancia il wallet di stato, Chivo Wallet, accumulando Bitcoin come riserva di valore, e prevedendo la distribuzione di 200 ATM nel paese. Inoltre, ha offerto ai propri cittadini un bonus di 30 dollari in Bitcoin al momento dell’iscrizione al wallet.

L’introduzione di questa legge prevede sin da subito che:

- Bitcoin può essere utilizzato per estinguere i debiti, senza limitazioni, in qualsiasi transazione;
- Bitcoin può essere accettato come pagamento per beni o servizi;
- qualsiasi pagamento di tasse può essere effettuato in Bitcoin;
- qualsiasi obbligo precedente espresso in dollari USA può essere pagato in Bitcoin;
- gli standard contabili continueranno a utilizzare il dollaro statunitense come valuta di riferimento;
- il governo fornirà un sistema che consentirà agli utenti di convertire automaticamente e istantaneamente i Bitcoin in dollari.

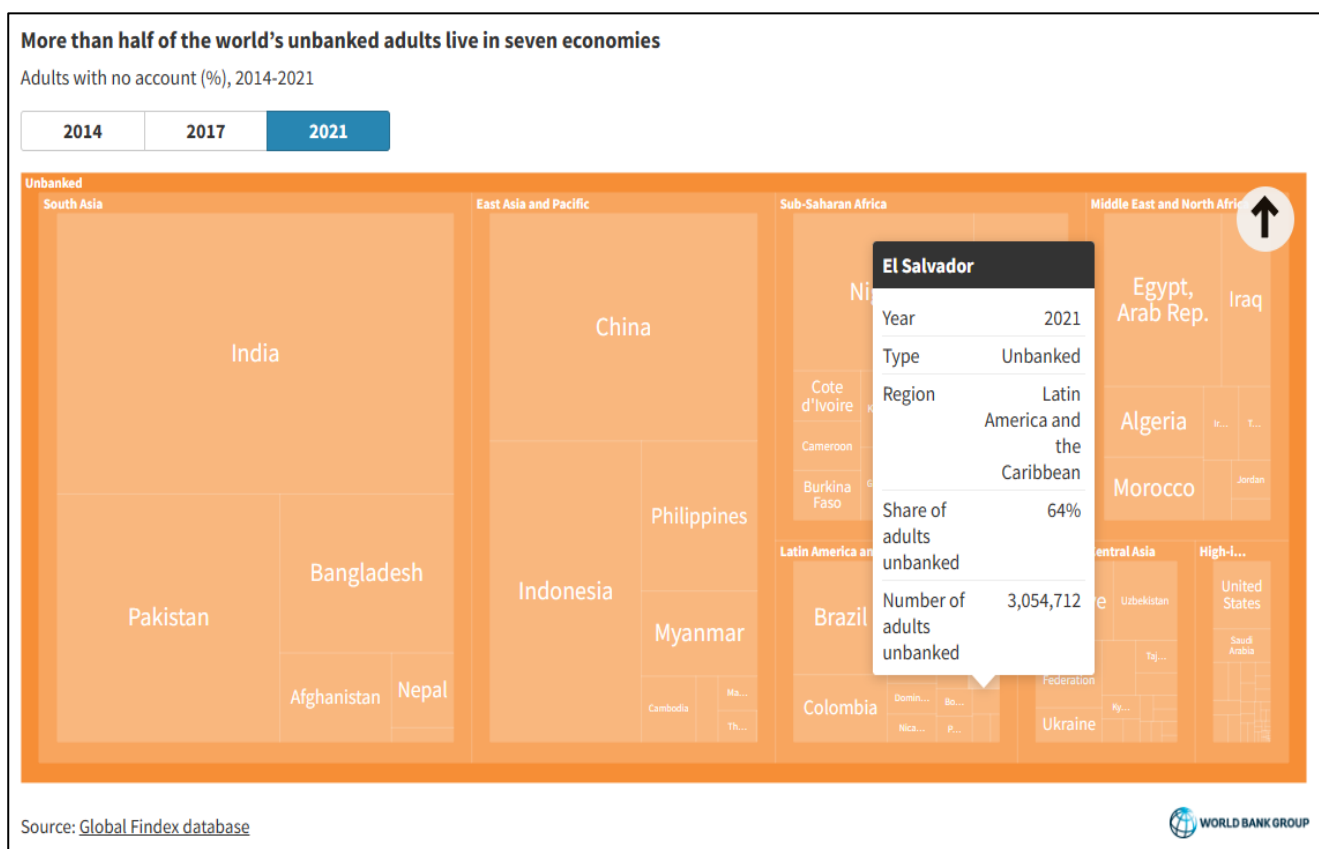
L'introduzione di questa nuova valuta è stata una scelta spinta principalmente da tre fattori:

1. Ridurre la dipendenza dal dollaro statunitense; Bitcoin permetterebbe al Paese di avere a disposizione una riserva di valore neutrale per i risparmi;
2. Ridurre il numero di *unbanked*. I dati mostrano che, nel 2021, il 64% della popolazione risultava non avere accesso ad un conto bancario e servizi finanziari<sup>27</sup>;
3. Aumentare l'efficienza delle rimesse internazionali; infatti, più del 20% del PIL salvadoregno deriva dalle rimesse estere,<sup>28</sup> il che implica possibili costi associati, che vanno dal 30 al 50% del

valore trasferito e difficoltà nella gestione del denaro.

A seguito di questa mossa, prontamente sono arrivati gli avvisi da parte del Fondo Monetario Internazionale (IMF), contrario ai piani del Presidente Bukele. L'IMF si è detto principalmente preoccupato per le possibili implicazioni macroeconomiche, finanziarie e legali di questa adozione.

Oltre all'introduzione della nuova valuta, è stato dato il via alla costruzione di una mining farm all'interno di una centrale geotermica, che permette di sfruttare l'energia prodotta dai vulcani attivi per effettuare sperimentazioni di mining di Bitcoin con lo scopo di raccogliere dati utili alla costruzione di un'infrastruttura produttiva nel prossimo futuro.



27

<https://www.worldbank.org/en/publication/globalfindex/interactive-executive-summary-visualization>

28

<https://data.worldbank.org/indicator/BX.TRF.PWKR.DT.G.D.ZS?locations=SV>

L'iniziativa di El Salvador si scontra con la realtà della popolazione locale, una popolazione per lo più povera che vive con meno di \$300 dollari al mese e un basso livello di educazione. Il successo dell'applicazione Chivo Wallet, che ha visto l'iscrizione di oltre 4 milioni di utenti, è da attribuire principalmente al bonus di \$30 dollari che veniva regalato in fase di iscrizione. Molti dei cittadini hanno convertito il bonus in dollari, come consente di fare l'app, e pochi hanno continuato ad utilizzarla per effettuare pagamenti in Bitcoin. Anche il numero di attività che accetta Bitcoin è basso: dai primi rilevamenti, solo il 20%. Nonostante questo, risultano continue transazioni effettuate tutt'oggi tramite Chivo, il che significa che molte persone, anche parte di quelle che precedentemente non avevano accesso ai sistemi finanziari, hanno ora la possibilità di detenere un mezzo con il quale effettuare pagamenti digitali ed inviare e ricevere denaro.

Il limite all'adozione di questa tecnologia è, come già scritto, il basso livello di educazione e di comprensione di questo nuovo strumento. Nonostante Bukele avesse promesso programmi di educazione per aiutare i cittadini ad avvicinarsi a Bitcoin e imparare ad utilizzare il wallet come strumento di pagamento di tutti i giorni, così non è stato. Invece, grazie ad un'associazione di volontari è nato "Mi Primer Bitcoin" il cui "obiettivo è quello di mettere gli studenti in condizione di fare il primo passo verso l'utilizzo di Bitcoin. Vogliamo dare l'esempio.

Mostrare piuttosto che raccontare. Rendere reale l'intangibile"<sup>29</sup>. Hanno iniziato portando corsi su Bitcoin e il suo utilizzo pratico presso due scuole, creando un vero e proprio diploma che i ragazzi possono conseguire superando un esame finale. Ora, l'obiettivo è quello di espandersi presso altre scuole e non solo, portare conoscenza e informazione anche ai cittadini. Insomma, stanno provando a fare ciò che il governo finora non ha fatto, al fine di aumentare l'adozione nel Paese.

Al di là delle difficoltà, Bukele sta cercando di trarre vantaggio da questa situazione cercando di richiamare Bitcoiner e imprenditori, proponendo una legge che detassa completamente l'innovazione tecnologica<sup>30</sup>, con l'obiettivo di attrarre capitale dall'estero.

Inoltre, riguardo non di poco conto, El Salvador ha rispettato il pagamento del prestito obbligazionario, in scadenza nel 2023, di \$800 milioni, contro le aspettative di molti che dichiaravano un possibile default del Paese. Certo è che, con più di duemila Bitcoin nelle casse dello Stato, un aumento del prezzo di Bitcoin oltre i livelli di novembre 2021 renderebbe molto al Paese, rafforzando enormemente la sua situazione finanziaria.

---

<sup>29</sup> <https://miprimerbitcoin.io/mision/>

<sup>30</sup> <https://twitter.com/nayibbukele/status/1639070248627208197>

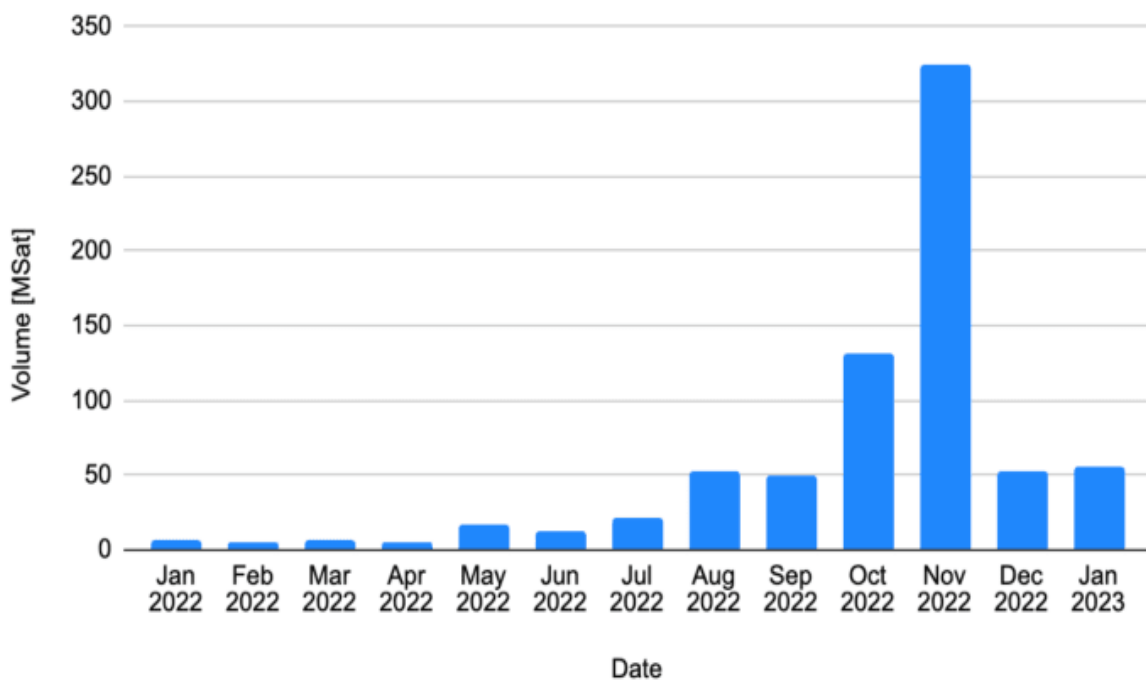
## 2.2 Guatemala e Costa Rica

Altri due esempi di paesi in cui i cittadini hanno iniziato ad adottare Bitcoin sono il Guatemala e il Costa Rica. Mentre in El Salvador l'adozione ha seguito un processo *top-down*, quindi è stata dettata dall'alto, questi due paesi hanno seguito un processo *bottom-up*.

Anche in Guatemala sussiste il problema degli *unbanked*, con il 60% della popolazione che non ha accesso ai servizi finanziari. Nasce così sulle sponde del lago Atitlan, a Panajachel, il progetto "Bitcoin Lake". L'obiettivo di questo progetto è di creare un'economia circolare alimentata da Bitcoin, mettendo a disposizione nuove soluzioni accessibili a tutti, sia ai negozianti, ma soprattutto a tutte quelle persone che sino ad

ora sono state escluse dal sistema finanziario. Il coinvolgimento dal basso della popolazione, mosso da Bitcoiner volontari, ha avuto effetti positivi, vedendo il coinvolgimento di oltre 60 attività, di cui il 90% accettava solo contanti e ora anche Bitcoin. In tutto il 2022 ci sono state oltre quattro mila transazioni per un volume di 7.39 Bitcoin (circa \$ 222.400 al cambio attuale)<sup>31</sup>. Spesso, in questi paesi, il motivo per cui carte di debito/credito, tantomeno le American Express, non vengono accettate non è dovuto solo dal fattore *unbanked*, per cui il proprietario di un'attività non possiede gli strumenti per poterle accettare, bensì, un'altra causa sono le elevate commissioni che le compagnie delle carte applicano ai negozianti, intorno all'8%<sup>32</sup>. Se comparate alle

### Volume 2022



<sup>31</sup> <https://bitcoinmagazine.com/culture/inside-guatemalas-bitcoin-lake>

<sup>32</sup> <https://asocialnomad.com/guatemala/atms-in-guatemala/#:~:text=In%20most%20countries%2C%20th>

[ere%20will.Guatemala%2C%20it%27s%20around%208%25.](https://www.willguatemala.com/it/2022/11/25/)

commissioni applicate ai pagamenti effettuati su *Lightning Network*<sup>33</sup>(LN), non c'è confronto: mediamente le *fee* (commissioni) su LN sono lo 0.1%.

Inoltre, ciò che serve per iniziare a ricevere ed inviare pagamenti con questa tecnologia è solo uno smartphone, una connessione ad internet ed installare un'app che funziona da wallet. Quindi, anche i costi iniziali a livello hardware sono nulli, a differenza di quanto normalmente richiesto dalle banche per l'installazione dei PoS.

Infine, anche in Guatemala sono stati avviati gli stessi corsi nati in El Salvador da "Mi Primer Bitcoin" con lo stesso obiettivo: educare la popolazione a questi nuovi strumenti e alle loro potenzialità.

Un progetto simile a quello guatemalteco è la "Bitcoin Jungle" in Costa Rica. Anche in questo caso nasce da un processo *bottom-up*, da alcuni ragazzi che hanno iniziato con il convincere alcune attività ad accettare Bitcoin come forma di pagamento. La missione della "Bitcoin Jungle" è quella di creare un'economia circolare basata su Bitcoin nel Triangolo d'Oro, che comprende Dominical, Uvita, Ojochal e Perez Zeledon. L'obiettivo è quello di creare una cittadella Bitcoin orizzontale che permetta ai Bitcoiner, siano essi locali, residenti a lungo termine o turisti, di utilizzare liberamente Bitcoin e la rete Lightning per tutte le loro esigenze di vita.

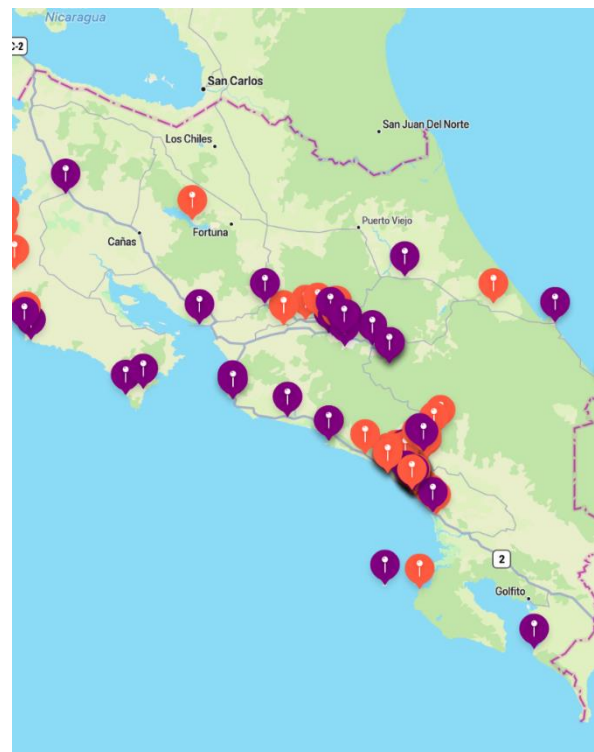
In questo caso si è iniziata a creare una vera e propria economia circolare dove i venditori al mercato vendono le materie prime ai

ristoratori in Bitcoin, i quali li accettano a loro volta dai clienti e pagano (almeno in parte) i loro impiegati in Bitcoin. Questi ultimi pagano beni e servizi, magari dagli stessi venditori al mercato, con i Bitcoin guadagnati.

Ci sono circa 150 attività che hanno iniziato ad accettare questa nuova valuta, e circa 90 sono posizionate nel Triangolo d'Oro.

Per agevolare l'adozione, hanno creato anche una rete di persone che convertono Bitcoin in contanti, in caso di necessità da parte di qualche venditore.

A livello normativo, non ci sono vincoli sulla tipologia di pagamento, il che facilita i negozianti. Infatti, in Costa Rica, la legge consente di accettare il pagamento in cambio di un bene concordato. Pertanto, se entrambe le parti concordano che si tratta di una forma di pagamento accettabile, è consentito.



<sup>33</sup> Lightning Network è il layer due di Bitcoin, progettato per consentire transazioni veloci e a basse commissioni

tra gli utenti ed è stato proposto come soluzione al problema di scalabilità di Bitcoin.

## 2.3 USA – Texas

Uno dei processi cardine del protocollo Bitcoin è il *mining*. Il termine richiama appositamente il minare, in quanto, come nelle miniere vengono estratti i metalli preziosi, anche in questo caso ad ogni blocco creato vengono generati nuovi Bitcoin, come sistema incentivante. Ma lo scopo del processo non è solo questo, anzi, il *mining* è il meccanismo che garantisce la sicurezza del sistema e permette il raggiungimento di un consenso a livello di rete senza l'intervento di un'autorità centrale.

Per ottenere questa ricompensa, i *miner* competono per risolvere un problema matematico complesso basato su un algoritmo di hash crittografico, utilizzando la potenza di calcolo dei loro hardware. La soluzione del problema, chiamata Proof-of-Work, viene inclusa nel nuovo blocco e rappresenta la prova che il *miner* ha impiegato un notevole potenza di calcolo. La

competizione per la soluzione dell'algoritmo Proof-of-Work per ottenere la ricompensa e il diritto di registrare le transazioni sulla blockchain è alla base del modello di sicurezza di Bitcoin.

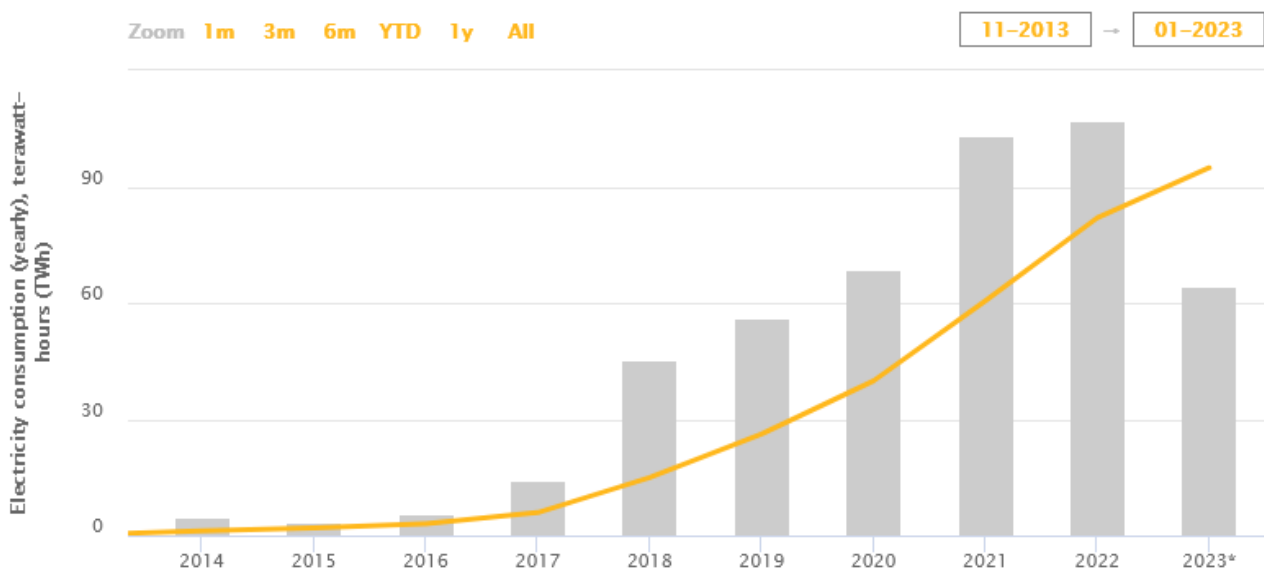
Se nel 2009 bastava un computer domestico per minare, dato il basso numero di componenti della rete, e quindi una bassa competizione, ora servono hardware specializzati per questo tipo di lavoro, gli ASIC. Con gli anni quella del *mining* è diventata un'industria estremamente competitiva, che richiede competenze e strumentazione specializzata per tale scopo e l'accesso a molta corrente elettrica a basso costo.

La quantità di energia richiesta è cresciuta esponenzialmente negli anni e, ad oggi, il consumo annuale stimato dal "Cambridge Bitcoin Electricity Consumption Index" è di 149 TWh, che rispetto al consumo energetico mondiale è lo 0.67% del totale<sup>34</sup>.

Molte *mining farm* erano situate in Cina, in quanto ricca di centrali idroelettriche e

### Total Bitcoin electricity consumption

Select an area by dragging across the lower chart



<sup>34</sup> <https://ccaf.io/cbnsi/cbeci/comparisons>

energia venduta a basso costo, ma, nel 2021, lo Stato ha deciso di bannare il *mining*, costringendo i *miner* ad andarsene e trovare nuovi paesi favorevoli per il loro business. Molti di loro traslocarono in America, in Texas, grazie all'elevata produzione di energia elettrica da fonti rinnovabili. Questo particolare è importante per i *miner*, in quanto la produzione di energia da fonti rinnovabili viene venduta ad un costo più basso, il che implica maggiori profitti per i *miner*.

Il consumo energetico delle *mining farm* è stimato intorno ai 2.5 GW, ma la stessa produzione è passata da 44.8 GW nel 2021 a 49.2 GW nel 2022<sup>35</sup>.

Ciò che risulta interessante, però, è come il *mining* stia dimostrando di essere una fonte di supporto alla griglia elettrica del paese. Infatti, i fornitori di corrente elettrica stipulano con i *miner* dei contratti di fornitura flessibile, in cui in caso di necessità, il surplus energetico viene indirizzato alla griglia elettrica e messo a disposizione della popolazione. Questa dinamicità è garantita dal fatto che gli ASIC possono essere spenti e riaccesi con facilità e risulta vantaggiosa un paese come il Texas in cui in certi periodi invernali ed estivi soffrono di grossi blackout dovuti ad una richiesta sovradimensionata a cui non si riesce a far fronte.

Proprio per questo motivo l'*Electric Reliability Council Of Texas* (ERCOT) nel suo report "Seasonal Assessment of Resource Adequacy for the ERCOT Region" (SARA), riferito all'inverno 2022-2023, ha introdotto nei suoi

conteggi anche il *mining* di Bitcoin come fonte da cui attingere per far fronte a casi estremi di richiesta energetica. Nel report è stata inserita la voce *Operational Co-located Resources with Large Flexible Loads (LFLs)* per riferirsi appunto a questa risorsa con carichi ampiamente flessibili, per un totale di 1.7 GW di cui possono usufruire in caso di picchi di domanda per l'inverno<sup>36</sup>.

Questo utilizzo del *mining* a supporto della rete elettrica è un esempio pratico di come Bitcoin si integri perfettamente nella produzione e nel bilanciamento della stessa. Il fatto che tutto ciò sia inserito nel bilancio aziendale e nella pianificazione della ERCOT, un'organizzazione che si occupa di fornitura elettrica nel Paese, dimostra l'applicabilità di questa soluzione.

---

<sup>35</sup> <https://app.electricitymaps.com/zone/US-TEX-ERCO>

<sup>36</sup> Seasonal Assessment of Resource Adequacy for the ERCOT Region, Winter 2022/23, p.2

## 2.4 Africa

Osservando la classifica *Global Crypto Adoption Index* del 2022 prodotta da Chainalysis si trovano tre paesi africani nella top 20: Nigeria all'undicesimo posto, Marocco al quattordicesimo e Kenya al diciannovesimo. Dunque, anche in Africa aumenta l'adozione delle criptovalute e, nonostante il volume di transazioni nell'Africa Sub-Sahariana rappresenti solo il 2% delle attività mondiali, mostra dati interessanti e una significativa penetrazione nelle attività finanziarie giornaliere di molte persone. Ma qual è la motivazione? Principalmente, gli alti volumi sono legati a trasferimenti verso questi paesi, tanto che nel periodo tra luglio 2021 – giugno 2022 i primi tre paesi in quest'area per valore ricevuto in criptovalute sono il Sud Africa con circa \$25 miliardi, seguito da Nigeria e Kenya, con quasi \$20 miliardi.

Anche questi Paesi sono colpiti da un forte tasso di *unbanked*, per fare un esempio in Nigeria rappresentano il 60% della popolazione, e di persone che lasciano il paese per andare a lavorare oltremare e inviano denaro alle proprie famiglie. In quest'ultimo caso, effettuare pagamenti verso paesi come la Nigeria, il Kenya o il Camerun può essere complicato e molto costoso in termini di commissioni, che possono raggiungere anche il 20%. Soluzioni come Bitcoin, grazie ad una delle sue caratteristiche fondamentali, ossia il non aver confini, consentono di inviare pagamenti da e verso qualsiasi parte del mondo, con

commissioni irrisorie. A volte è possibile pure trarne un profitto: *"Ray described one Kenyan expat he knew who had to pay €200 for every €1,000 she tried to send home from Europe. Ray was able to help that woman use Paxful to buy Bitcoin, sell it to another user for Kenyan shillings via M-PESA, a Kenyan payments network, which the woman could then transfer directly to her family. 'She actually ended up making a 4% profit rather than paying 20% in fees because the user she transacted with was willing to pay a premium for the Bitcoin,' said Ray."*<sup>37</sup>.

Un altro caso d'uso sono le transazioni commerciali. Bitcoin e le altre criptovalute danno la possibilità alle imprese locali di superare i limiti stringenti imposti dal sistema bancario centrale e di effettuare pagamenti verso altri stati, come gli USA e la Cina.

Facendo un focus su Bitcoin, in Africa trova un'applicazione molto interessante il *minigrids*. Oltre 600 milioni di persone sono prive di rete elettrica, maggiormente nell'Africa Sub-Sahariana. Per dare un'idea della situazione, viene consumata più energia elettrica in Norvegia che in tutta l'Africa. In molte zone remote, la domanda di elettricità risulta troppo bassa per giustificare investimenti necessari alla costruzione di centrali e reti elettriche. La miglior soluzione a questo tipo di problema sono le *minigrids*, piccole centrali che generano fino a 1 MW di energia. Anche in questo caso, però, a fronte del capitale iniziale d'investimento, i ritorni dall'elettricità venduta sono lenti ed irregolari. Proprio per questo, l'integrazione di piccole

---

<sup>37</sup> The 2022 Geography of Cryptocurrency Report, pp.73-80

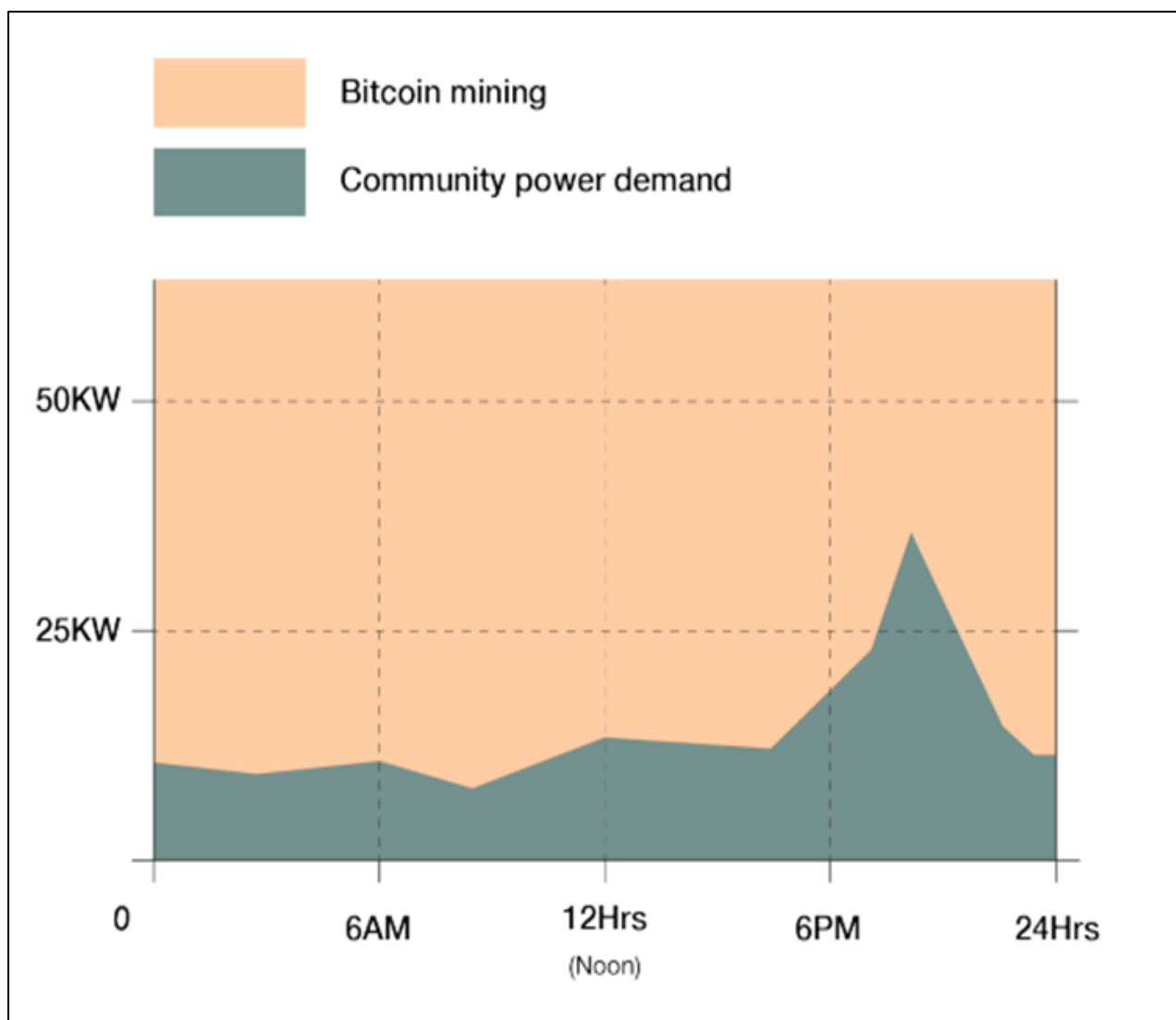


*mining farm* alle *minigrid* permetterebbero di:

- sfruttare l'energia che altrimenti andrebbe sprecata in quei momenti in cui la domanda è bassa o nulla mentre, quando è alta, di liberare spazio garantendola alla popolazione;
- garantire una stabilità finanziaria agli investitori grazie ad una domanda prevedibile e consistente;
- essere posizionate ovunque, in quanto agnostiche alla posizione.

Inoltre, le *mining farm* giocherebbero tre ruoli cruciali, data la flessibilità nell'utilizzo dell'energia elettrica:

- *buyer of first resort*, comprando l'energia quando non c'è domanda;
- *buyer of last resort*, comprandola solo quando non serve a nessun altro;
- *grid-balancer of last resort*, equilibrato la domanda-risposta per mantenere la *minigrid* sempre stabile.



La chiave di un'infrastruttura con un legame energia-Bitcoin sta nel fatto che sarebbe basata sulla comunità, fornita localmente, agnostica alla posizione, accessibile economicamente e, soprattutto, per tutti i cittadini. Un punto debole c'è, ovvero richiede un *rate* di utilizzo minimo, il quale dipende dai costi della strumentazione utilizzata per minare Bitcoin, dall'efficienza delle macchine e dal valore di Bitcoin, che garantirebbe parte del profitto.

Molti villaggi in Africa sono tagliati fuori per mancanza di corrente, nonostante sia un paese potenzialmente ricchissimo di energia rinnovabile. Una soluzione di questo tipo darebbe la possibilità di sfruttare queste risorse della natura, permettendo l'accesso ad una fonte di energia a tutti coloro che oggi ne sono privi e ad un prezzo ridotto, grazie al guadagno ulteriore che si ricaverebbe attraverso il *mining* e l'eventuale vendita di Bitcoin. Questo è quello che sta facendo Gridless in Kenya, una compagnia di *mining* in Africa orientale, finanziando la costruzione e la gestione di alcuni data center Bitcoin in comunità rurali e stipulando accordi con HydroBox, compagnia idroelettrica africana. Tre di questi data center sono già operativi.

# CONCLUSIONI

di Gianluca Aurelio e Giorgio Cardile

L'orizzonte degli eventi delle Central Bank Digital Currencies e delle criptovalute lascia intravedere un grande potenziale. Rimane essenziale bilanciare tali sviluppi con la tutela della privacy dei cittadini e la protezione dei loro diritti. Ipotizziamo due scenari.

Nel primo, la mancata (o insufficiente) tutela della privacy ha reso semplice il monitoraggio di ogni transazione CBDC.

La CBDC traccia ogni singolo pagamento, e tutte le informazioni vengono conservate dalla banca centrale. Significa che ogni centesimo di quel conto è tracciabile e monitorato.

Una possibile deriva distopica (che trova però dei riscontri anche nel presente) è il rapporto che potrebbe iniziare tra un sistema di social scoring e il monitoraggio delle spese dei cittadini tramite i dati acquisiti dalle transazioni CBDC.

Un altro possibile profilo di rischio è la permanenza di tutte le informazioni (come vengono spesi i soldi provenienti da conti CBDC) in un unico luogo (nel nostro scenario, la banca centrale) pone dei rischi alla sicurezza in caso di *data breach*.

Infine, l'utilizzo esclusivo delle CBDC non andrebbe incontro alla risoluzione delle diverse problematiche legate agli *unbanked* e allo spostamento di denaro a livello

internazionale. I limiti di accesso ai conti bancari, al credito e agli strumenti finanziari tradizionali non verrebbero superati. L'unica differenza riscontrabile sarebbe uno spostamento del 'controllore', che passerebbe dalle banche private locali alla banca centrale di riferimento. Inoltre, come oggi risulta difficile e oneroso inviare denaro verso determinate aree del mondo, allo stesso modo lo sarà con le CBDC: ogni paese avrà il proprio sistema, che si dovrà integrare con gli altri. I pagamenti saranno sottoposti agli stessi (o maggiori) controlli, provocando tempi lunghi per l'incasso e costi comunque elevati per l'invio.

Nel secondo caso, le criptovalute sono ormai diffuse tanto quanto la valuta nazionale e quasi ogni persona ha ormai diversi portafogli che usa per gli scopi più disparati, dal fare la spesa, al dividersi il conto in pizzeria, al rinnovo automatico degli abbonamenti e al pagamento delle rette universitarie. Bitcoin esiste ancora e convive con la moneta locale, i servizi finanziari iniziano a offrire servizi correlati e, soprattutto, tutti i cittadini, in qualsiasi Paese, riescono ad avere accesso ad un conto. Sono stati sviluppati nuovi *layer* sopra Bitcoin che consentono la gestione di diversi servizi, sia di pagamento, sia di gestione di contratti, di certificazione di

documenti, dell'identità digitale. Insomma, il protocollo Bitcoin vede uno sviluppo simile a quello di internet, con il suo *core* che si ossifica per svolgere alla perfezione le funzionalità cardine e, sopra di esso, vengono sviluppati nuovi livelli, che interagiscono con quello base, ciascuno con finalità distinte. Ad esempio, come Lightning Network per pagamenti più rapidi ed economici.

Gli Stati si avvalgono dei *miner* per integrare la griglia di rete elettrica con le *mining pool*, migliorando la capacità e la gestione della domanda e dell'offerta, diversificando le fonti e prediligendo quelle rinnovabili. Vengono sviluppate *minigrids* distribuite nei Paesi in via di sviluppo che consentono di elettrificare piccoli villaggi precedentemente privi di servizi.

Dunque, questa tecnologia trova un equilibrio e utilizzo all'interno della società. Grazie alla sua natura, garantisce maggiore accesso e indipendenza finanziaria, privacy e sicurezza alle persone, facilita e velocizza i pagamenti, soprattutto quelli internazionali, e trova applicazioni anche al di fuori dell'ambito dei pagamenti.

# BIBLIOGRAFIA E SITOGRAFIA

- Gallardo R., *Inside bitcoin lake: lessons from my months as a volunteer with guatemala's groundbreaking project*, Bitcoin Magazine, 2023, <https://bitcoinmagazine.com/culture/inside-guatemalas-bitcoin-lake>, ultima consultazione 05/07/2023.
- Carter S., *How to Use ATMs in Guatemala – Finding the Cheapest ATMS*, ASocialNomad, 2016, <https://asocialnomad.com/guatemala/atms-in-guatemala/#:~:text=In%20most%20countries%2C%20there%20will,Guatemala%2C%20it%27s%20around%208%25>, ultima consultazione 05/07/2023.
- Cambridge Bitcoin Electricity Consumption Index, <https://ccaf.io/cbnsi/cbeci/comparisons>, ultima consultazione 24/06/2023.
- Chainalysis (2023) Crypto Crime Report 2023, disponibile sul [loro sito](#).
- Chainalysis, The 2022 Geography of Cryptocurrency Report, 2022.
- Electric Reliability Council of Texas, Seasonal Assessment of Resource Adequacy for the ERCOT Region (SARA) - Winter 2022/23, 2022.
- Electricity Maps, <https://app.electricitymaps.com/zone/US-TEX-ERCO>, ultima consultazione 13/07/2023.
- Mi Primer Bitcoin, Misión, <https://miprimerbitcoin.io/mision/>, ultima consultazione 10/07/2023
- Nakamoto S., Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.
- PWC, El Salvador's law: a meaningful test for Bitcoin, 2021.
- Transparency International (2022), Corruption perception index 2022, disponibile sul [loro sito](#).
- The World Bank (2000). Anticorruption in Transition: Contribution to the Policy Debate. World Bank Publications. ISBN 9780821348024, p. 3 (disponibile su [Researchgate](#)).
- The World Bank, The Global Findex Database 2021, <https://www.worldbank.org/en/publication/globalfindex/interactive-executive-summary-visualization>, ultima consultazione 08/07/2023.
- The World Bank, Personal remittances, received (% of GDP) - El Salvador, <https://data.worldbank.org/indicator/BX.TRF.PWKR.DT.GD.ZS?locations=SV>, ultima consultazione il 08/07/2023.
- Twitter, <https://twitter.com/nayibbukele/status/1639070248627208197>, ultima consultazione il 10/07/2023.

# HANNO COLLABORATO A QUESTO NUMERO



## **GIANLUCA AURELIO**

Laureato in Scienze Criminologiche, appassionato di informatica, Bitcoin e di blockchain, e affascinato dalla storia dell'attivismo digitale. Analista Junior dell'Associazione Italiana Analisti di Intelligence e Geopolitica (AIAIG) e collaboratore di AMIStaDeS.

<https://www.linkedin.com/in/gianlucaaurelio/>



## **GIORGIO CARDILE**

Laureato in giurisprudenza, praticante avvocato presso uno studio di diritto amministrativo e dei settori regolati, membro dell'European Center for Space Law e del European Centre for Space Economy and Commerce. Collabora con AMIStaDeS come Analista per l'area Spazio.

<https://www.linkedin.com/in/giorgiocardile/>

## **REALIZZAZIONE GRAFICA**

**ANDREA SPEZIALE**  
SMM & Graphic Editor  
AMIStaDeS



<https://www.linkedin.com/in/andrea-speziale-240147a8/>

## **COORDINAMENTO**

**CLAUDIA  
CANDELMO**  
Segretario Generale  
AMIStaDeS



<https://www.linkedin.com/in/claudia-candelmo-7b655428/>

## **PROGETTO EDITORIALE**

**ILARIA DANESI**  
Assistant Business  
Development  
AMIStaDeS



<https://www.linkedin.com/in/ilariadanesi14/>



# L'ORIZZONTE DEGLI EVENTI

**Quaderni geopolitici e analisi giuridiche**

NUMERO 13 - LUGLIO 2023

**BITCOIN E CRIPTOVALUTE:  
LIMITI E POTENZIALITÀ**

ISSN: 2724-2315



EDITO DA

**Centro Studi AMIStaDeS**

[www.amistades.info](http://www.amistades.info)

[info@amistades.info](mailto:info@amistades.info)

Via Cesena 22, 00182 Roma