POLITECNICO DI TORINO
Repository ISTITUZIONALE

Bitcoin e Blockchain

Original
Bitcoin e Blockchain / Bracciali, A., Errati, L., Gavioli, N.. - ELETTRONICO. - (2024).

Availability:
This version is available at: 11583/3017626 since: 2026-11-06T14:54:36Z

Publisher:
De Cifris Press

Published
DOI:

Terms of use:

This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

Publisher copyright

(Article begins on next page)

17 November 2026

DE CIFRIS KOINE
Book Series
Volume VI

Bitcoin & Blockchain

DE CIFRIS KOINE
Series Editorial Board

Editor-in-Chief
Massimiliano Sala,
De Componendis Cifris, Presidente
Managing editor
Antonino Alì,
Università di Trento, Professore

Editors
Gianira Nicoletta Alfarano,
KU Leuven, Researcher
Elena Berardini,
Université de Bordeaux, Chaire de Professeur Junior
Martino Borello,
Université Paris 8, Maître de Conférences
Alessio Caminata,
Università di Genova, Ricercatore
Michela Ceria,
Politecnico di Bari, Ricercatrice
Michele Ciampi,
The University of Edinburgh, Chancellor's Fellow
Roberto Civino,
Università dell'Aquila, Ricercatore
Veronica Cristiano,
Telsy SpA, Cryptographer
Daniele Friolo,
Università di Roma "La Sapienza", Ricercatore
Tommaso Gagliardoni,
Kudelski Security, Cryptographer and Scientist
Giovanni Giuseppe Grimaldi,
Università di Napoli Federico II, Ricercatore
Annamaria Iezzi,
Université Grenoble Alpes, Maîtresse de Conférences
Michela Iezzi,
Banca d'Italia, Ricercatrice

Carla Mascia,
DataKrypto, Ricercatrice
Barbara Masucci,
Università di Salerno, Professoressa
Carmine Monetta,
Università di Salerno, Ricercatore
Andrea Monti,
Università di Chieti, Docente
Marco Moraglio,
Università dell'Insubria, Ricercatore
Marzio Mula,
Universität der Bundeswehr München, Ricercatore
Nadir Murru,
Università di Trento, Professore
Giancarlo Rinaldo,
Università di Messina, Ricercatore
Francesco Romeo,
Università di Cassino e del Lazio Meridionale, Ricercatore
Carlo Sanna,
Politecnico di Torino, Ricercatore
Paolo Santini,
Università Politecnica delle Marche, Ricercatore
Daniele Taufer,
Katholieke Universiteit Leuven, Ricercatore
Lea Terracini,
Università di Torino, Professoressa
Marco Timpanella,
Università di Perugia, Ricercatore
Ilaria Zappatore,
Université de Limoges, Maîtresse de Conférences

DE CIFRIS KOINE
Book Series

De Cifris Koine è una collana editoriale curata da De Cifris Press, marchio dell'associazione nazionale De Componendis Cifris dedicata allo studio e alla divulgazione della crittografia e delle discipline correlate.

Questa collana rappresenta un punto di riferimento per la comunità crittografica italiana, offrendo una panoramica delle ricerche e delle innovazioni nel campo. Attraverso la pubblicazione degli atti di conferenze e workshop, De Cifris Koine fornisce non solo approfondimenti scientifici, ma anche contributi divulgativi, mettendo in luce i progressi e le attività dei principali esponenti in questo ambito.

La serie abbraccia un ampio spettro di argomenti, estendendosi oltre la crittografia stessa per includere le sue molteplici applicazioni e intersezioni con altre discipline. Tra queste, si annoverano la teoria dei codici, vari rami della matematica come l'algebra, la teoria dei numeri e la geometria, l'informatica con un focus particolare sulla cybersecurity e sull'informatica teorica, nonché l'ingegneria elettrica, le telecomunicazioni, la storia e gli aspetti legali legati alla crittografia.

Gli articoli pubblicati in questa collana sono accettati in tre lingue: italiano, inglese e francese.

La periodicità della pubblicazione è trimestrale.

De Cifris Koine is a book series published by De Cifris Press, publishing house of the national association De Componendis Cifris, whose activities focus on cryptography and related topics. De Cifris Koine volumes form the voice of the Italian cryptographic community, as they collect communications from both scientific and educational events and summaries of papers of its members and of their activities. In particular, De Cifris Koine hosts conference and workshop proceedings, including short abstracts.

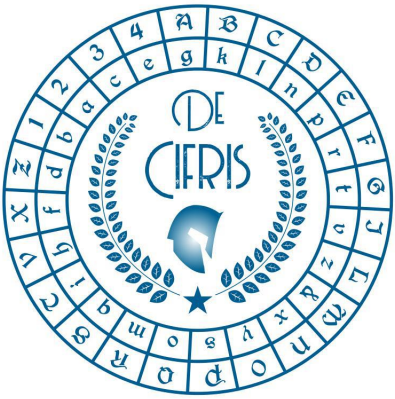
Topics covered in De Cifris Koine volumes relate to cryptography and its applications to and connections with other disciplines, as for example coding theory, maths (mainly algebra, number theory and geometry), computer science (mainly cyber security and theoretical computer science), electronic engineering, telecommunication engineering, history of cryptography and law.
Accepted articles are either in Italian, English or French.
Volumes are published quarterly.

La De Cifris Koine est une collection publiée par la De Cifris Press de l'association nationale italienne De Componendis Cifris. Elle est consacrée à l'étude et à la diffusion de la cryptographie et des disciplines connexes.

Cette collection est une référence importante pour la communauté cryptographique italienne, offrant une vue d'ensemble de la recherche et des innovations dans ce domaine. Grâce à la publication d'actes de conférences et de groupes de travail (workshops), la De Cifris Koine fournit non seulement des contributions scientifiques académiques, mais aussi des contributions à destination du grand public, mettant en lumière les progrès et les activités des principaux acteurs et des principales actrices du domaine.

Les articles de cette collection couvrent un large éventail de sujets allant de la cryptographie à ses nombreuses applications et intersections avec d'autres disciplines. On y retrouve notamment la théorie des codes, diverses branches des mathématiques telles que l'algèbre, la théorie des nombres et la géométrie, l'informatique, avec un accent sur la sécurité informatique et l'informatique théorique, ainsi que le génie électrique, les télécommunications et les aspects juridiques de la cryptographie. Les articles soumis à la De Cifris Koine sont acceptés en italien, anglais et français. La fréquence de publication est trimestrielle.

Bitcoin & Blockchain

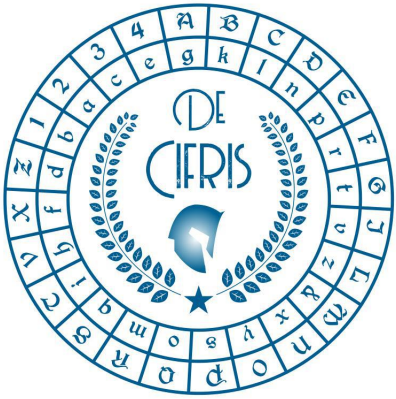


Edited by:

- *Andrea Bracciali*,
  Professore associato,
  Università di Torino, IT

- *Leonardo Errati*,
  Studente di dottorato,
  Politecnico di Torino, IT

- *Norberto Gavioli*,
  Professore associato,
  Università dell'Aquila, IT



Pubblicazione trimestrale di proprietà dell'associazione nazionale di crittografia
De Componendis Cifris

Autorizzazione del Tribunale di Milano in data 23 - 02 - 2024
Num. R.G. 1315/2024 Num. Reg. Stampa 22
ISSN: 3034-9796 ISBN: 979-12-81863-05-7
I diritti d'autore sono riservati.
Editore: De Componendis Cifris APS.
Marchio Editoriale: De Cifris Press.
Direttore responsabile: Massimiliano Sala
Redazione: Antonino Alì, Nadir Murru
Luogo di pubblicazione: Via Gianfranco Zuretti 34 - 20125 Milano
e-mail: editorial@decifris.it
Stampa in proprio
Numero 6 - Pubblicato il Maggio 2025

PREFACE

Con le crittovalute (e la tecnologia blockchain) l'impatto della crittografia non si limita più a un ambito squisitamente tecnologico, ma investe l'economia, la società e, quindi, la politica. Gli editor del volume, Andrea Bracciali Leonardo Errati e Norberto Gavioli, hanno raccolto contributi di natura molto diversa tra loro, proprio per tentare di catturare questa poliedricità. Il tema è troppo vasto per una trattazione sistematica, ma sono sicuro che il lettore apprezzerà l'ampio respiro che caratterizza questo volume.

With cryptocurrencies (and the underlying blockchain technology), the impact of cryptography is no longer confined to a purely technological sphere, but extends to the economy, society and, consequently, politics.

The editors of this volume, Andrea Bracciali Leonardo Errati e Norberto Gavioli, have brought together contributions that differ greatly in nature, precisely in an attempt to capture this multifaceted character. The subject is too broad to allow for a systematic treatment, but I am confident that readers will appreciate the wide-ranging perspective that characterizes this volume.

Avec les cryptomonnaies (et la technologie blockchain qui les sous-tend), l'impact de la cryptographie ne se limite plus à un domaine purement technologique, mais s'étend à l'économie, à la société et, par conséquent, à la politique.

Les éditeurs de cet ouvrage, Andrea Bracciali Leonardo Errati e Norberto Gavioli, ont réuni des contributions de nature très diverse, précisément dans le but de tenter de saisir ce caractère protéiforme. Le sujet est trop vaste pour faire l'objet d'un traitement systématique, mais je suis convaincu que le lecteur appréciera l'ampleur de vue qui caractérise cet ouvrage.

Massimiliano Sala
Editor in Chief
De Cifris Koine

Table of Contents

Part I
Introduction

Cryptography and Bitcoin 2
Andrea Bracciali, Leonardo Errati, and Norberto Gavioli

Part II
Bitcoin

Bitcoin oltre il denaro: genealogia tecnopolitica e ambivalenza della sovranità algoritmica 18
Denis Roio

Scalare Bitcoin oltre la Timechain 37
Gianluca Cappiello

Wallet e indirizzi in Bitcoin 53
Enrico Zangirolami

zk-STARKs and Computational Integrity in Bitcoin Layer-2 Protocols 69
Bianca Rampazzo

Attacco ad un sottogruppo di chiavi del sistema Bitcoin 85
Domenica Sogiorno

Part III
Applicazioni

Le stablecoin nella rivoluzione silenziosa del denaro: tra geopolitica e finanza. 101
Vincenzo Vespri

Civic blockchain: tokenized economies supporting local communities 126
Cristina Viano, Irene Domenicale, Sowelu Avanzo, and Claudio Schifanella

AI e Blockchain: convergenza tra intelligenza artificiale e fiducia digitale 141
Davide Carboni

Part IV
Aspetti Legali

La disciplina delle cripto-attività nell'UE e nel Regno Unito: Scenari Regolatori a Confronto 157
Cristina Poncibò, Luigi Cantisani

Part I
Introduction

Cryptography and Bitcoin

Andrea Bracciali [1], Leonardo Errati [2], and Norberto Gavioli [3]

[1] Università degli Studi di Torino
[2] Politecnico di Torino
[3] Università degli Studi dell'Aquila

Abstract. Bitcoin is the result of decades of cryptographic research, failed attempts, and insights accumulated outside traditional academic circuits. This contribution retraces the historical trajectory that made Bitcoin possible, introducing along the way the fundamental cryptographic structures on which it rests: elliptic curves, hash functions, Merkle trees, proof of work, and zero-knowledge proofs. We provide a narrative thread connecting all subsequent contributions.

"Every informed person needs to know about Bitcoin because it might be one of the world's most important developments."
- Leon Louw, author and policy advisor

1 Introduction to the volume

Modern cryptography has succeeded in transforming decades of mathematical theory, from computational complexity to abstract algebra, into concrete foundations underpinning much of today's digital infrastructure. Bitcoin and blockchain technology are perhaps the most interesting example of this transformation: a system in which digital signatures, cryptographic hash functions, distributed consensus mechanisms, and game theory combine to produce something novel [36].

Bitcoin is a cryptographic object: a shared, immutable ledger with no central authority [1]. But also a phenomenon which has transcended the boundaries of the technical community to reshape law, monetary economics, institutional politics, and perhaps even philosophy. Understanding Bitcoin therefore requires a multidisciplinary perspective: mastery of the underlying cryptography is not enough if one ignores the governance implications of a permissionless network, or the legal tensions surrounding the classification of digital assets, or the sociotechnical dynamics that made its emergence possible at that particular historical moment.

De Cifris Koine – BITCOIN & BLOCKCHAIN
https://doi.org/10.69091/koine/vol-6-B01

The roots of that moment reach back to the cypherpunk culture of the 1990s. The movement, founded in 1992 by Eric Hughes, Timothy May, and John Gilmore, had already grasped that cryptography was not merely a technical tool but a form of political resistance [26, 32].

This volume was conceived to offer the cryptographic community, and more broadly anyone wishing to engage with the subject rigorously, a reference that takes all these dimensions into account without sacrificing any of them.

Overview of the Volume

The volume is organised in four parts.

Part I is dedicated to the introduction, with the aim of providing the reader with the context needed to approach the subsequent chapters.

Part II is perhaps the heart of the book. The contributions collected here explore Bitcoin from multiple perspectives: a technopolitical genealogy reconstructing the historical conditions of its emergence; an analysis of scalability mechanisms beyond the timechain; a detailed examination of the structure of wallets and addresses [1]; an introduction to ZK-SNARK systems as applied to Bitcoin; and finally a cryptanalytic study of attacks on subgroups of keys in the Bitcoin system.

Part III broadens the scope to applications: from stablecoins as an emerging monetary phenomenon, to civic blockchains in support of local communities, to the convergence of artificial intelligence and distributed ledger technologies.

Part IV addresses the legal dimension, with a contribution dedicated to the legal classification of digital assets under current positive law; a question far from settled, and of growing practical relevance.

Intended Audience

This volume is addressed primarily to graduate students and doctoral researchers in mathematics, computer science, and engineering who already have a working familiarity with the basic concepts of modern cryptography [10]. It is not an introductory guide to Bitcoin: readers will find neither elementary explanations of how a blockchain works nor instructions on how to purchase cryptocurrencies. The assumption is that the reader wishes to understand Bitcoin *in depth*: its cryptographic mechanisms, design choices, technical limitations, and social and legal implications.

The volume will also be of use to researchers and practitioners seeking to orient themselves in the current landscape of blockchain, as well as to legal scholars and policy makers who wish to engage with a technically grounded treatment of the legal aspects of digital assets.

How to Read This Volume

The chapters are conceived as self-contained contributions and may be read independently, although they follow a logical progression from theory to practice and from the technical to the legal. Readers with a predominantly mathematical interest may wish to begin with Part II, while those searching for a more applied or legal standpoint may find it helpful to read Part III first.

Each article is accompanied by a bibliography that allows the reader to pursue each topic further. In a field evolving as rapidly as this one, some of the open problems discussed in the contributions may already have been resolved by the time of reading: yet the foundations presented here remain solid, and constitute a durable basis for anyone wishing to continue exploring this space.

2 The Making of Bitcoin

2.1 Simple Problems Require Complex Solutions

The history of cryptography applied to digital payment systems begins long before 2008 with a simple but difficult question: is it possible to transfer value digitally without relying on a central intermediary?

The problem is strikingly non-trivial. Digital money is information, and information can be copied. Anyone who possesses a file representing "one coin" could, in principle, send it to two different recipients. This is the so-called *double-spending problem*. Banks solve it by maintaining a central ledger and acting as arbiters. But a central ledger is also a potential point of control, of censorship, and of failure. The question that obsessed the *cypherpunks* of the 1990s was different: does a cryptographic solution exist? how can we build trust digitally?

The answer took decades to assemble. Every component of Bitcoin existed before 2008 in some form: hash functions, digital signatures, Merkle trees, proof of work. The whitepaper by Satoshi Nakamoto [36] assembled them into a system that solves the double-spending problem without a trusted party. Understanding Bitcoin means understanding how and why this was done.

2.2 The Crypto Wars: When Cryptographers Were Smugglers

To understand why the cypherpunks were building what they were building, one must understand what was happening decades before.

The 1990s were a period of open conflict between governments and cryptographers over who controls the tools of privacy. The United States government classified strong cryptography as a *munition* under the International Traffic in Arms Regulations

(ITAR). Exporting software with keys longer than 40 bits, laughably short and even then known to be breakable in mere hours, required a State Department licence. The NSA, which had long dominated cryptographic research through classified channels, had been confronted in the 1970s with two blows:

- the publication of the Data Encryption Standard (DES) [37], which forced a public debate about key lengths and government interference in standards.
- Diffie and Hellman's *New Directions in Cryptography* [17] in 1976, the paper that introduced public-key cryptography, and proposed the concept of *digital signatures*.

The cypherpunk movement, loosely organised around a mailing list founded in 1992 by Eric Hughes, Timothy May, and John Gilmore, operated on a simple conviction: *privacy is not a privilege but a precondition for freedom, and cryptography is its technical expression* [27].

Their intellectual program was articulated by Hughes in *A Cypherpunk's Manifesto*: "cypherpunks write code".[27]. The tools of privacy had to be built, not negotiated. Timothy May's *Crypto Anarchist Manifesto* [31], distributed at the first cypherpunk meeting, went further: in 1988, long before the web existed, he predicted that cryptographic protocols would "alter the nature of government regulation, the ability to tax and control economic interactions".

The conflict came to a head with episodes that remain formative for anyone working in applied cryptography.

The first one was the **Clipper chip** affair [30]. In 1993, the Clinton administration proposed mandatory adoption of a government-designed encryption chip for telecommunications, with a built-in *key escrow* mechanism: every encrypted communication would be decryptable by law enforcement upon presentation of a court order. The cryptographic community responded with a mixture of technical analysis and outrage. Matt Blaze from AT&T Bell Labs published a paper demonstrating a flaw in the escrow protocol [8]. The proposal was abandoned not through legislation, but through market rejection and sustained technical criticism.

The second episode was the **prosecution of Phil Zimmermann**. In 1991, Zimmermann released *Pretty Good Privacy* (PGP) [56], a freely available implementation of public-key encryption for email, built on RSA. When PGP spread outside the United States via the early internet, the government opened a criminal investigation for illegal munitions export. The investigation ran for three years. It was eventually dropped, in part because Zimmermann published the PGP source code as a *book*, and exporting a book was protected by the First Amendment. A printed listing of C code crossed the border legally; the same code on a floppy disk did not.

Meanwhile, a computer science professor named Daniel Bernstein was fighting his own battle. In 1995, Bernstein wanted to publish an encryption algorithm he had developed, called Snuffle. The State Department told him he needed an export

licence to post the source code on the internet. Bernstein sued, arguing that source code was speech protected by the First Amendment. *Bernstein v. United States* [6] wound through the courts for years, producing a landmark Ninth Circuit ruling in 1999 that source code is indeed protected speech. The ITAR regulations were subsequently revised.

The war, for a moment, seemed won. But the Crypto Wars resumed in the 2010s with the Snowden revelations [22], which confirmed that the NSA had systematically compromised cryptographic standards. Allegedly, this included the random number generator Dual_EC_DRBG [14], which had been pushed into the NIST standards process and contained a suspected backdoor. The lesson was clear: trust in cryptographic infrastructure cannot be delegated. It must be earned through open standards, public scrutiny, reproducible implementations, and the kind of adversarial peer review that only an open community can provide.

2.3 A Graveyard of Good Ideas

Bitcoin emerged from a specific intellectual lineage of people who tried to solve the same problem.

David Chaum's *DigiCash* [13], developed through the 1980s and commercialised in the early 1990s, was the first serious attempt. Chaum introduced *blind signatures*, a technique that allows a bank to sign a token without seeing its content, preserving the anonymity of the payer while preventing double-spending. The cryptography was elegant and original. The architecture was not: DigiCash required Chaum's company, *DigiCash Inc.*, to operate the mint, and when the company filed for bankruptcy in 1998, the currency disappeared with it.

Nick Szabo's *Bit Gold* [47], proposed in 1998, came so close to the Bitcoin architecture that it remains a subject of speculation whether Szabo is Nakamoto. Bit Gold described a chain of proof-of-work puzzles, each referencing the previous one via a hash, with ownership tracked through public keys. It was never implemented; Szabo could not solve the double-spending problem without a trusted registry.

Wei Dai's *b-money* [15], proposed the same year on the cypherpunks mailing list, introduced the idea of a distributed ledger maintained by a peer-to-peer network in which every participant keeps a copy of all account balances. Nakamoto explicitly cited b-money in the Bitcoin whitepaper.

The missing piece was consensus. Adam Back's *Hashcash* [2], designed in 1997 as an anti-spam mechanism for email, contributed the proof-of-work primitive that Bitcoin would adopt as its consensus engine. Back's insight was that requiring a sender to perform a small computation, in this case finding a value whose hash meets a target, makes spam economically unattractive without inconveniencing

legitimate users. The computation is cheap once, expensive in bulk. Bitcoin made the computation expensive once, and made that expense the basis of security.

Hal Finney, a cryptographer who had contributed to PGP and was present at the first cypherpunk meeting, refined the idea with *Reusable Proofs of Work* (RPOW) [20] in 2004, creating tokens that could be passed between users. He was also the recipient of the first Bitcoin transaction in history, on 12 January 2009, when Nakamoto sent him ten bitcoin. Finney died in 2014 of ALS.

What Nakamoto assembled in 2008 was the architecture that had eluded everyone else: a distributed ledger with no central operator, in which double-spending is prevented not by trust but by thermodynamics, and in which consensus is reached not by voting but by proof of work. The Bitcoin whitepaper [36] is nine pages long.

3 Cryptographic Foundations

3.1 Hash Functions: The Backbone of the System

A *cryptographic hash function* $H : \{0,1\}^* \to \{0,1\}^n$ maps an input of arbitrary length to a fixed-length digest. Three properties make it cryptographically useful:

- **Preimage resistance**: given y, it is computationally infeasible to find x such that $H(x) = y$.
- **Second preimage resistance**: given x, it is infeasible to find $x' \neq x$ such that $H(x) = H(x')$.
- **Collision resistance**: it is infeasible to find any pair (x, x') with $x \neq x'$ and $H(x) = H(x')$.

Bitcoin uses two hash functions. **SHA-256** [38], standardised by NIST, used in address generation, in the proof-of-work puzzle, in Merkle tree construction, and in transaction identifiers. **RIPEMD-160** [18], developed in the European RIPE project, composed with SHA-256 in the address generation pipeline (Section 3.5).

The collision resistance of SHA-256 is why the blockchain is tamper-evident. Altering any transaction in a past block changes its hash, which changes the hash of the following block, cascading forward in an avalanche that invalidates the entire subsequent chain. This property was already formalised by Haber and Stornetta in 1991 [25] as a mechanism for timestamping digital documents. Nakamoto's blockchain is an extension of that idea: the Haber-Stornetta paper is cited in the whitepaper, and its authors hold the curious distinction of having three of the eight non-Nakamoto citations in a document that changed financial history.

3.2 Proof of Work: The Cost of Trust

Back's Hashcash [2] posed the following problem: find a value x such that $H(x) \leqslant T$, where T is a target threshold. Because a good hash function behaves like a random oracle, there is no smarter strategy than brute force: try values of x until one works. The expected number of attempts is $2^{256}/T$, which can be tuned by adjusting T. The result is a *proof of work*, a certificate that a certain amount of computation was performed, verifiable in a single hash evaluation.

In Bitcoin, the puzzle is: find a *nonce* n such that

$$H(H(\text{block header} \,\|\, n)) \leqslant T,$$

where the block header commits to the previous block's hash, a Merkle root of transactions, and a timestamp. The target T is adjusted every 2016 blocks (roughly two weeks) to maintain an average block time of ten minutes, regardless of how much hash power joins or leaves the network. At time of writing, the difficulty is such that the global network performs on the order of 10^{20} hash evaluations per second [9]: more evaluations per second than there are grains of sand on Earth.

Proof of work solves the double-spending problem as follows. To replace a confirmed transaction with a conflicting one an attacker must recompute all subsequent blocks faster than the honest network extends the chain. With less than 50% of the global hash rate, this is computationally infeasible in any practical timeframe[4]. Trust is replaced by thermodynamics: the longest chain represents the most work, and work costs energy.

This comes at a heavy price. The energy consumption of Bitcoin mining is substantial, and a subject of legitimate debate [16]. Alternative consensus mechanisms exist. *Proof of Stake* (PoS), adopted by Ethereum in 2022 [19], replaces computational work with economic stake: validators are chosen proportionally to the cryptocurrency they lock as collateral, with misbehaviour penalised by *slashing* the stake. PoS eliminates the energy cost but introduces different security assumptions; in particular, the system is secure as long as a majority of stake is held by honest validators, a condition whose robustness under adversarial conditions is an active area of research [12].

3.3 Merkle Trees: Committing to a Set

A *Merkle tree* [33] is a binary tree in which each leaf contains the hash of a data block, and each internal node contains the hash of its two children. The *Merkle root* is a single hash that commits to the entire dataset: any modification to any leaf produces a different root, by collision resistance.

[4] Attacking this by achieving miner majority is the so-called 51% *attack*.

In Bitcoin, the Merkle root of a block's transaction set is included in the block header, binding the proof of work to a specific set of transactions. A miner who finds a valid nonce cannot then swap transactions into the block without invalidating the nonce itself. The Merkle structure also enables *SPV* (Simplified Payment Verification) [36]: a lightweight client can verify that a transaction is included in a block by downloading only a *Merkle proof* rather than the full block. This only consists of the $O(\log n)$ sibling hashes along the path from the leaf to the root.

3.4 Elliptic Curves and Digital Signatures

Ownership of bitcoin is established through *digital signatures*. The underlying mathematics is the theory of elliptic curves over finite fields, independently proposed for cryptographic use by Koblitz [29] and Miller [34] in 1985.

An elliptic curve over a prime field $\mathbb{F}_p$ is the set of points (x, y) satisfying $y^2 = x^3 + ax + b \pmod{p}$. These points, together with a point at infinity $\mathcal{O}$ serving as identity, form an abelian group under a geometric addition law. The security of elliptic curve cryptography rests on the *elliptic curve discrete logarithm problem* (ECDLP): given points P and $Q = kP$, recovering the scalar k is computationally infeasible for appropriately chosen parameters. The advantage over RSA is efficiency: the same security level requires dramatically shorter keys, which is why ECDLP became the standard for constrained environments and, eventually, for Bitcoin.

Bitcoin uses the curve `secp256k1`, defined by $y^2 = x^3 + 7$ over $\mathbb{F}_p$ with

$$p = 2^{256} - 2^{32} - 977,$$

a Mersenne-like prime chosen for efficient modular reduction. The group order q is a 256-bit prime, ensuring that no proper subgroup is large enough to be cryptographically useful to an attacker. This property is directly exploited, in the other direction, in the subgroup attack described by Sogiorno in this volume.

Bitcoin originally used **ECDSA** (Elliptic Curve Digital Signature Algorithm) [28]. ECDSA produces a signature (r, s) from a message hash and a private key; this is a cryptographic protocol ensuring that anyone holding the public key can verify the signature, while being unable to recover the private key. A first structural weakness of ECDSA is that combining signatures from multiple parties requires interaction and multiple round trips, making collaborative signatures quite complex. A subtler one is that signature generation requires a fresh random nonce k for each signing operation; reusing k for two different messages reveals the private key. This is not a theoretical concern: the software in the PlayStation 3 was broken in 2010 because it used a constant k in ECDSA signing.

The **Taproot** upgrade [53–55], activated in November 2021, introduced **Schnorr signatures** [44]. Schnorr signatures satisfy a *linearity* property: given public keys $K_1, \ldots, K_n$, one can construct an aggregate public key $K_{\text{agg}} = \sum_i c_i K_i$ and a single aggregate signature valid for all parties simultaneously, via the **MuSig2** protocol [40]. This reduces the on-chain footprint of multi-signature transactions and improves privacy, since aggregate signatures are indistinguishable from single-party signatures.

3.5 From Keys to Addresses

A Bitcoin address is a processed hash of a public key. This accounts for compactness, error detection, and versioning. Starting from a public key $K = (K_x, K_y)$, the legacy address generation pipeline is:

$$\text{address} = \text{Base58Check}(\texttt{0x00} \,\|\, \text{RIPEMD-160}(\text{SHA-256}(\texttt{0x04} \,\|\, K_x \,\|\, K_y))) \,.$$

The double hashing provides defence in depth: even if SHA-256 were broken, an attacker would still face RIPEMD-160. The `Base58Check` encoding introduces a 4-byte checksum and avoids visually ambiguous characters (`0`, `O`, `I`, `l`), a decision that reflects the protocol's attention to human factors. Modern address formats use **Bech32** and **Bech32m** encoding [51, 52], which offer stronger error detection and are optimised for QR codes.

3.6 Hierarchical Deterministic Wallets

Managing one key pair per transaction is operationally impractical. BIP 32 [49] introduced *hierarchical deterministic* (HD) wallets: a mechanism to derive an entire tree of key pairs from a single secret seed, using HMAC-SHA512 as the derivation function. The seed is typically encoded as a human-readable sequence of 12 or 24 words from a standardised wordlist, as specified by BIP 39 [42].

This decision trades mathematical elegance for memorability. The HD wallet tree is navigated by *derivation paths* of the form

```
m/purpose'/coin_type'/account'/change/index
```

where the apostrophe denotes *hardened derivation*: a mode in which child keys cannot be derived from the parent's public key alone, providing an additional security boundary. Standard path assignments are codified in BIP 44 (legacy P2PKH), BIP 49 (Nested SegWit), BIP 84 (Native SegWit), and BIP 86 (Taproot) [41, 48, 43, 50].

3.7 Zero-Knowledge Proofs

In Bitcoin every transaction, every address, every amount is visible to anyone. This is a deliberate design choice, as transparency enables verification, but it is also a

privacy liability. The entire field of *confidential transactions* and *zero-knowledge proofs* (ZKPs) can be understood as the attempt to reconcile these two requirements.

A zero-knowledge proof system [21] allows a *prover* to convince a *verifier* that a statement is true without revealing any information beyond the truth of the statement itself. Formally, a proof system must be *complete* (an honest prover always convinces the verifier), *sound* (a dishonest prover cannot convince the verifier of a false statement except with negligible probability), and *zero-knowledge* (the verifier learns nothing beyond the validity of the statement). The framework was introduced by Goldwasser, Micali, and Rackoff in a paper that also introduced the concept of *interactive proofs*, which won them the Turing Award in 2012.

zk-SNARKs (Succinct Non-interactive ARguments of Knowledge) are ZKPs that produce proofs of constant or logarithmic size, verifiable in time sublinear in the size of the witness, i.e. the computation that the prover claims to have performed correctly [23]. They power the privacy guarantees of Zcash [5] and are increasingly relevant to Bitcoin's Layer 2 ecosystem. **zk-STARKs** (Scalable Transparent ARguments of Knowledge) [4] eliminate the trusted setup, a one-time ceremony in which secret randomness must be generated and then irreversibly destroyed; if compromised, an adversary can forge proofs undetected. These, however, rely on collision-resistant hash functions and making them post-quantum secure under standard assumptions instead. Their integration with Bitcoin's second layer is explored in detail by Rampazzo in this volume.

4 What Comes Next?

4.1 The Post-Quantum Boogeyman

Quantum computing introduces a discontinuity into classical security. Choosing longer keys will not save us; this requires replacing the mathematical problems on which the whole field rests.

Shor's algorithm [45], if run on a sufficiently large and fault-tolerant quantum computer, solves the discrete logarithm problem in polynomial time. This breaks ECDSA and Schnorr simultaneously.

Grover's algorithm [24] provides a quadratic speedup for unstructured search, halving the effective security of hash functions: SHA-256's 256-bit output provides 128 bits of post-quantum security, a comfortable margin [7].

The implications for Bitcoin are asymmetric. The hash-based components (proof of work, Merkle trees, address generation) are largely resilient. Unspent outputs whose public keys have not yet been revealed are protected by the hash of the

public key; recovering the private key would require breaking both SHA-256 and RIPEMD-160. The signature scheme, on the other hand, is an acute problem. Every published public key is potentially vulnerable to a quantum attacker. This creates a stratification of risk. In particular, *pay-to-public-key* (P2PK) outputs, used in the earliest blocks including Satoshi's own coinbase transactions, expose the raw public key directly and offer no hash-based protection.

The threat is not immediate. Estimates for a cryptographically relevant quantum computer range from a decade to several decades [35], and the field has a history of optimistic timelines that were subsequently revised. NIST's Post-Quantum Cryptography standardisation process, concluded in 2024 [39], produced **ML-KEM** for key exchange and **ML-DSA** and **SLH-DSA** for digital signatures. Hash-based signatures (SLH-DSA) are the most conservatively secure: their security reduces to collision resistance of the underlying hash function alone. However, they produce significantly larger signatures, straining Bitcoin's block space. The path to post-quantum is technically clear but socially complicated: it requires consensus on a replacement signature scheme, a migration mechanism for existing funds, and a community governance process that has historically required years even for uncontroversial changes [46].

Like the Crypto Wars before it, the post-quantum transition will be a test of whether a decentralised community can coordinate a migration of existential importance on a timeline it does not control.

4.2 Beyond Bitcoin: Chains, Contracts, and CBDCs

Bitcoin was a proof of concept that inspired a wave of successors. Ethereum, launched in 2015 by Vitalik Buterin with a whitepaper written when he was nineteen [11], extended the blockchain model with a Turing-complete virtual machine, making arbitrary computation verifiable on-chain. This enabled *smart contracts*, self-executing programs whose terms are directly written into code, and with them an entire ecosystem of decentralised finance, tokenisation, and programmable money.

At the opposite end of the spectrum, central banks worldwide are developing *Central Bank Digital Currencies* (CBDCs) [3]: digital versions of fiat currency issued directly by a central authority. The cryptographic toolkit is similar: hash functions, digital signatures, sometimes zero-knowledge proofs for privacy. However, the architecture is inverted. Where Bitcoin is trustless by design, a CBDC is trust-maximising by design: the central bank is the single source of truth, the authority that issues and potentially freezes or programmes the currency. The contrast illuminates how much of Bitcoin's architecture is not a technical necessity but a political choice.

Between these poles lies a spectrum of experimentation: permissioned blockchains for interbank settlement, tokenised securities on public chains, Layer 2 protocols that move computation off-chain while anchoring security to Bitcoin's proof of work. The cryptographic foundations are shared; the implications for trust, privacy, and governance diverge sharply.

4.3 A Note on What Follows

The contributions collected in this volume assume the material surveyed here. The volume opens with Roio, who situates Bitcoin within a broader perspective on the innovation it introduces, offering the reader a point of entry beyond the purely technical. Cappiello analyses the scalability constraints of Bitcoin's base layer and the Layer 2 protocols (Lightning Network, Ark, BitVM) designed to circumvent them; all of these rely on the hash and signature primitives described above. Zangirolami provides a detailed treatment of HD wallets and derivation standards, building directly on the BIP 32 framework. Rampazzo develops the theory of zk-STARKs and their application to Bitcoin's second layer. Sogiorno presents a subgroup attack on Bitcoin's key space, whose mathematical substrate is the ECDLP and the group structure of `secp256k1`. Vespri examines stablecoins as an emerging monetary and geopolitical phenomenon. Viano et al. and Carboni explore applications and convergences: blockchain for local communities and the intersection with artificial intelligence. Poncibò and Cantisani situate the entire ecosystem within the emerging European and British regulatory frameworks.

These are chapters in a longer story that began with a mailing list, a handful of failed prototypes, a professor who published a book to avoid a weapons charge, and the hope that mathematics and technology could do what institutions would not.

Andrea Bracciali, Leonardo Errati & Norberto Gavioli
Editors of Volume VI
De Cifris Koine

References

1. Andreas M. Antonopoulos. *Mastering Bitcoin: Programming the Open Blockchain*. O'Reilly Media, Sebastopol, CA, 2nd edition, 2017.
2. Adam Back. Hashcash — a denial of service counter-measure. `http://www.hashcash.org/papers/hashcash.pdf`, 2002.
3. Bank for International Settlements. Central bank digital currencies: Foundational principles and core features. Technical Report Report No. 1, BIS, 2021.
4. Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev. Scalable, transparent, and post-quantum secure computational integrity. IACR ePrint 2018/046, 2018.
5. Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. Zerocash: Decentralized anonymous payments from bitcoin. In *IEEE Symposium on Security and Privacy*, pages 459–474, 2014.
6. Daniel J. Bernstein. Bernstein v. United States: Background. `https://cr.yp.to/export.html`, 1999.
7. Daniel J. Bernstein and Tanja Lange. Post-quantum cryptography. In *Encyclopedia of Cryptography and Security*. Springer, 2017.
8. Matt Blaze. Protocol failure in the escrowed encryption standard. In *ACM Conference on Computer and Communications Security*, pages 59–67, 1994.
9. Blockchain.com. Bitcoin hash rate. `https://www.blockchain.com/charts/hash-rate`, 2024.
10. Dan Boneh and Victor Shoup. A Graduate Course in Applied Cryptography. `https://toc.cryptobook.us/`, 2023. Draft textbook, freely available online. Accessed: 2025.
11. Vitalik Buterin. Ethereum: A next-generation smart contract and decentralized application platform. `https://ethereum.org/en/whitepaper/`, 2014.
12. Vitalik Buterin. Why proof of stake. `https://vitalik.ca/general/2020/11/06/pos2020.html`, 2020.
13. David Chaum. Blind signatures for untraceable payments. In *Advances in Cryptology – CRYPTO 1982*, pages 199–203. Plenum Press, 1983.
14. Stephen Checkoway, Matthew Fredrikson, Ruben Niederhagen, Adam Everspaugh, Matthew Green, Tanja Lange, Thomas Ristenpart, Daniel J. Bernstein, Jake Maskiewicz, and Hovav Shacham. On the practical exploitability of Dual EC DRBG in TLS implementations. In *USENIX Security Symposium*, pages 319–335, 2014.
15. Wei Dai. b-money. `http://www.weidai.com/bmoney.txt`, 1998.
16. Alex de Vries. Revisiting bitcoin's carbon footprint. *Joule*, 6(3):498–502, 2022.
17. Whitfield Diffie and Martin Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.
18. Hans Dobbertin, Antoon Bosselaers, and Bart Preneel. RIPEMD-160: A strengthened version of RIPEMD. In *Fast Software Encryption – FSE 1996*, volume 1039 of *LNCS*, pages 71–82. Springer, 1996.
19. Ethereum Foundation. The merge. `https://ethereum.org/en/upgrades/merge/`, 2022.
20. Hal Finney. Reusable proofs of work. `https://nakamotoinstitute.org/finney/rpow/`, 2004.
21. Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, 18(6):186–208, 1989.

22. Glenn Greenwald. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. Metropolitan Books, 2014.
23. Jens Groth. On the size of pairing-based non-interactive arguments. In *Advances in Cryptology – EUROCRYPT 2016*, volume 9666 of *LNCS*, pages 305–326. Springer, 2016.
24. Lov K. Grover. A fast quantum mechanical algorithm for database search. In *ACM Symposium on Theory of Computing*, pages 212–219, 1996.
25. Stuart Haber and W. Scott Stornetta. How to time-stamp a digital document. *Journal of Cryptology*, 3(2):99–111, 1991.
26. Eric Hughes. A Cypherpunk's Manifesto. `https://nakamotoinstitute.org/library/cypherpunk-manifesto/`, 1993. Published March 9, 1993. Accessed: 2025.
27. Eric Hughes. A cypherpunk's manifesto. `https://nakamotoinstitute.org/library/cypherpunk-manifesto/`, 1993.
28. Don Johnson, Alfred Menezes, and Scott Vanstone. The Elliptic Curve Digital Signature Algorithm (ECDSA). *International Journal of Information Security*, 1(1):36–63, 2001.
29. Neal Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177):203–209, 1987.
30. Steven Levy. *Crypto: How the Code Rebels Beat the Government—Saving Privacy in the Digital Age*. Viking, 2001.
31. Timothy C. May. The crypto anarchist manifesto. Distributed at the Crypto '88 conference; published on the Cypherpunks mailing list November 22, 1992. `https://nakamotoinstitute.org/library/crypto-anarchist-manifesto/`, 1988.
32. Timothy C. May. The Crypto Anarchist Manifesto. `https://nakamotoinstitute.org/library/crypto-anarchist-manifesto/`, 1988. Distributed at the Crypto '88 conference; published on the Cypherpunks mailing list November 22, 1992. Accessed: 2025.
33. Ralph C. Merkle. A digital signature based on a conventional encryption function. In *Advances in Cryptology – CRYPTO 1987*, volume 293 of *LNCS*, pages 369–378. Springer, 1988.
34. Victor S. Miller. Use of elliptic curves in cryptography. In *Advances in Cryptology – CRYPTO 1985*, volume 218 of *LNCS*, pages 417–426. Springer, 1985.
35. Michele Mosca. Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*, 16(5):38–41, 2018.
36. Satoshi Nakamoto. Bitcoin whitepaper. *URL: https://bitcoin.org/bitcoin.pdf*, 9:15, 2008.
37. National Bureau of Standards. Data encryption standard. Technical Report FIPS PUB 46, NBS, 1977.
38. National Institute of Standards and Technology. Secure hash standard (SHS). Technical Report FIPS PUB 180-4, NIST, 2015.
39. National Institute of Standards and Technology. Post-quantum cryptography standards (FIPS 203, 204, 205). `https://csrc.nist.gov/projects/post-quantum-cryptography`, 2024.
40. Jonas Nick, Tim Ruffing, and Yannick Seurin. MuSig2: Simple Two-Round Schnorr Multi-Signatures. In *Advances in Cryptology – CRYPTO 2021*, volume 12825 of *Lecture Notes in Computer Science*, pages 189–221. Springer, 2021.
41. Marek Palatinus and Pavol Rusnak. BIP 44: Multi-account hierarchy for deterministic wallets. Technical report, Bitcoin Improvement Proposal, 2014.

42. Marek Palatinus, Pavol Rusnak, Aaron Voisine, and Sean Bowe. BIP 39: Mnemonic code for generating deterministic keys. Technical report, Bitcoin Improvement Proposal, 2013.
43. Pavol Rusnak. BIP 84: Derivation scheme for P2WPKH based accounts. Technical report, Bitcoin Improvement Proposal, 2017.
44. Claus-Peter Schnorr. Efficient Signature Generation by Smart Cards. *Journal of Cryptology*, 4(3):161–174, 1991.
45. Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *IEEE Symposium on Foundations of Computer Science*, pages 124–134, 1994.
46. Iain Stewart. Committing to quantum resistance: A slow defence for bitcoin against a fast quantum computing attack. Royal Society Open Science, 5(6), 2018.
47. Nick Szabo. Bit gold. `https://nakamotoinstitute.org/library/bit-gold/`, 1998.
48. Daniel Weigl. BIP 49: Derivation scheme for P2WPKH-nested-in-P2SH based accounts. Technical report, Bitcoin Improvement Proposal, 2016.
49. Pieter Wuille. BIP 32: Hierarchical deterministic wallets. Technical report, Bitcoin Improvement Proposal, 2012.
50. Pieter Wuille. BIP 86: Deterministic wallet addresses for taproot. Technical report, Bitcoin Improvement Proposal, 2020.
51. Pieter Wuille and Greg Maxwell. BIP 173: Base32 address format for native v0–16 witness outputs. `https://github.com/bitcoin/bips/blob/master/bip-0173.mediawiki`, 2017.
52. Pieter Wuille and Greg Maxwell. BIP 350: Bech32m format for v1+ witness addresses. `https://github.com/bitcoin/bips/blob/master/bip-0350.mediawiki`, 2021.
53. Pieter Wuille, Jonas Nick, and Tim Ruffing. BIP340: Schnorr Signatures for secp256k1. `https://github.com/bitcoin/bips/blob/master/bip-0340.mediawiki`, 2020.
54. Pieter Wuille, Jonas Nick, and Anthony Towns. BIP 341: Taproot: Segwit v1 sigpubkey scripts. Technical report, Bitcoin Improvement Proposal, 2020.
55. Pieter Wuille, Jonas Nick, and Anthony Towns. BIP342: Validation of Taproot Scripts. `https://github.com/bitcoin/bips/blob/master/bip-0342.mediawiki`, 2020.
56. Philip R. Zimmermann. *The Official PGP User's Guide*. MIT Press, 1995.

Part II
Bitcoin

Bitcoin oltre il denaro: genealogia tecnopolitica e ambivalenza della sovranità algoritmica

Denis Roio

Fondazione PlanB, Lugano

Abstract. Questo saggio indaga l'emergenza di Bitcoin quale fenomeno di *soggettivazione collettiva*, individuandone l'origine in un momento di rottura (*καιρος*) legato alla crisi della presunta neutralità delle istituzioni finanziarie tradizionali. Questa crisi di neutralità, incombenza storicamente manifesta nei meccanismi di competizione del sistema finanziario, ha inesorabilmente catalizzato l'urgenza di strumenti decentralizzati per il trasferimento di beni economici. La mia analisi assume una prospettiva *biopolitica*, interrogando i processi attraverso cui una moltitudine distribuita ha sostituito il monopolio della violenza con la partecipazione algoritmica. L'innovazione contabile della *partita tripla* mediante firma digitale distribuita non costituisce mero progresso tecnico, bensì una mutazione nei dispositivi di governo della circolazione del valore, laddove il corpo sociale si fa esso stesso garante dell'autenticazione transazionale.

Con questa mia ricerca evidenzio come Bitcoin abbia infranto un'interdizione culturale di lunga durata, il cosiddetto **taboo del denaro**, attraverso la dimostrazione pratica di alternative sistemiche: lo faccio anche ripercorrendo traiettorie biografiche che incarnano forme di resistenza che eccedono la dimensione tecnologica, articolando pratiche di vita nelle quali la competenza crittografica si converte in impegno per l'autodeterminazione comunitaria entro spazi di conflitto e di sottrazione a governamentalità soggetta al monopolio.

Ad oggi i processi di sussunzione corporativa del fenomeno Bitcoin ne hanno amplificato degli aspetti e ridotto altri. Questo articolo aiuta a riconoscere le contraddizioni insite nelle molteplici strumentalizzazioni del progetto, ammettendo come la sovranità algoritmica sia esposta a forme di appropriazione che ne tradiscono l'ethos originario.

Tuttavia, proprio nell'interrogazione di tali tradimenti si individua la persistenza di una forza costitutiva irriducibile, quella di un dispositivo che ha inesorabilmente alterato le leggi fisiche che da secoli governano la produzione, l'autenticazione e la circolazione del denaro, lasciando aperta la possibilità di derive imprevedibili e di riappropriazioni comunitarie che eccedono tanto l'apologetica finanziaria quanto la sua demonizzazione.

De Cifris Koine – BITCOIN & BLOCKCHAIN
https://doi.org/10.69091/koine/vol-6-B02

1 Introduzione

Bitcoin va compreso non solo come innovazione monetaria, ma come rottura storica del monopolio fiduciario. Mettendo in discussione chi possa emettere, validare e trasferire valore senza ricorrere a intermediari sovrani o corporativi, il protocollo investe il rapporto tra moneta, fiducia, codice e sovranità. L'ipotesi di questo articolo è che Bitcoin abbia così infranto un'interdizione culturale di lunga durata, il taboo del denaro, rendendo progettuali funzioni fino ad allora attribuite a istituzioni centralizzate.

Questa apertura non produce tuttavia un esito univoco. Se rende possibile la sperimentazione anti-intermediaria, espone anche il protocollo e le tecnologie derivate a cattura economica, opacità tecnica e derive autocratiche. Per esaminare tale ambivalenza assumo una prospettiva genealogica e tecnopolitica: colloco Bitcoin nella storia della crittografia, delle culture hacker e cypherpunk, delle reti peer-to-peer e dei conflitti sulla neutralità dei pagamenti; considero inoltre mining, ledger condivisi e smart contract come dispositivi che redistribuiscono capacità di partecipazione, validazione e controllo.

Uso il termine decentralizzazione in senso analitico, non come sinonimo di libertà o democrazia. Esso può indicare almeno tre distribuzioni distinte: quella topologica, relativa alla presenza di una pluralità di nodi senza un unico punto di arresto; quella funzionale, relativa alla ripartizione delle operazioni di verifica e registrazione; quella politica, relativa alla possibilità effettiva dei partecipanti di influire sulle regole e sull'evoluzione del sistema. Questi livelli non coincidono necessariamente. Una rete può essere distribuita sul piano tecnico e restare concentrata nel mining, nello sviluppo del software, nelle interfacce di accesso o nella proprietà delle risorse. La decentralizzazione va quindi valutata come configurazione concreta di poteri e dipendenze, non come proprietà binaria o garanzia normativa [4, 2].

Con sovranità algoritmica non intendo invece un potere autonomamente esercitato dagli algoritmi, né la scomparsa dello Stato o della decisione umana. Il concetto designa la ricollocazione di funzioni tradizionalmente sovrane entro una infrastruttura programmabile: stabilire quali transazioni siano valide, ordinare una storia condivisa, regolare l'accesso, applicare automaticamente una regola e definire le procedure con cui essa può essere aggiornata. Questa autorità non appartiene al codice isolatamente, ma all'assemblaggio formato da protocollo, nodi, miners, sviluppatori, utenti, incentivi e infrastrutture materiali. È "algoritmica" perché una parte delle regole assume forma eseguibile e vincola anticipatamente l'azione; è "sovrana" perché tali regole decidono che cosa possa valere come operazione, prova e stato legittimo del sistema [22, 27].

I due concetti descrivono dunque aspetti diversi dello stesso problema. La decentralizzazione interroga dove siano collocate le capacità di validare, decidere e interrompere il sistema; la sovranità algoritmica interroga quali poteri siano esercitati attraverso il protocollo, da quali attori e con quali possibilità di contestazione. Una

architettura distribuita può rendere queste funzioni più partecipate e resistenti alla censura, ma può anche renderle opache, asimmetriche o difficili da modificare. È questa ambivalenza, e non una presunta neutralità del codice, a costituire il centro dell'argomentazione.

La genealogia critica non ricerca un'origine pura né ricostruisce una dottrina lineare, ma analizza le condizioni di emergenza e i rapporti di potere che rendono possibile un fenomeno storico [13]. Il contributo non offre quindi una rassegna generale delle interpretazioni di Bitcoin, comprese quelle legate alla tradizione austriaca, ma segue i passaggi in cui la moneta si ricompone come questione di infrastruttura, fiducia e governance. Bitcoin appare così come catalizzatore della crisi di fiducia negli intermediari e come tentativo di ridisegnare le condizioni tecniche della cooperazione sociale [21, 20, 16].

In questo senso Bitcoin può essere letto come una forma storicamente specifica di esodo dalle pratiche monetarie ufficiali: non una fuga dall'ordine economico, ma la costruzione di uno spazio in cui emissione, trasferimento e verifica del valore vengono riprogettati fuori dalla mediazione bancaria ordinaria. Tale processo si iscrive nella più lunga digitalizzazione dell'economia e nella sedimentazione di pratiche critiche verso la finanziarizzazione [15].

Questo articolo si sviluppa in quattro passaggi. Ricostruisce anzitutto il *καιρός* politico del blocco finanziario a WikiLeaks e la crisi della presunta neutralità dei pagamenti. Esamina poi l'autenticazione distribuita e il trasferimento di funzioni sovrane nel protocollo. Segue quindi l'espansione dal nucleo monetario di Bitcoin alle piattaforme in cui il problema si sposta verso la governance. Infine considera decentralizzazione, privacy e leggibilità del codice come terreni di negoziazione istituzionale e politica.

La tesi complessiva è che Bitcoin inauguri una sovranità algoritmica ambivalente. Rendendo il denaro pensabile come bene comune e infrastruttura progettuale, trasferisce il conflitto sul disegno delle regole e sulle forme di potere che esse favoriscono. Non si tratta quindi di stabilire se tali infrastrutture siano in sé emancipative o autoritarie, ma di comprendere come vi si confrontino autodeterminazione collettiva, mutualità infrastrutturale, finanziarizzazione e comando tecnico [4, 11, 7].

2 Genealogia: dal taboo del denaro al *καιρός* di WikiLeaks

La genealogia di Bitcoin non comincia con la sua apparizione pubblica, ma con una costellazione di pratiche e saperi che ne rendono possibile l'emersione. La crittografia come branca matematica, le culture hacker, l'immaginario cypherpunk e le reti peer-to-peer preparano il terreno per pensare il denaro non più come prerogativa esclusiva dello Stato o del sistema bancario, ma come problema tecnico, politico e organizzativo. In questa lunga preistoria, Bitcoin non appare come un accidente isolato, bensì come il punto in cui una serie di tensioni sedimentate trova finalmente una forma operativa [21].

Questa preistoria conta perché consente di vedere meglio che cosa realmente si rompe nel 2008–2011. Non si rompe solo un monopolio tecnico, ma un'intera immagine della moneta come dispositivo sottratto alla progettazione diffusa. In altre parole, il protocollo di Bitcoin non introduce semplicemente un nuovo strumento: ridefinisce il campo di ciò che può essere immaginato, discusso e sperimentato dal basso. La moneta cessa di apparire come funzione naturalmente riservata a stati, banche centrali e apparati fiduciari consolidati, e diviene un dispositivo di difesa dalla censura finanziaria [21].

L'origine di Bitcoin va letta come emergenza di un fenomeno di soggettivazione collettiva. Questo lessico evita due riduzioni speculari: da un lato la lettura puramente tecnica del protocollo, dall'altro la sua riduzione a ideologia monetaria.

Bitcoin non è solo un software e non è solo un discorso. È il punto di condensazione di una moltitudine distribuita, nel senso di pluralità cooperante che non si lascia ridurre né a popolo unitario né a semplice somma di individui, che sperimenta un'altra forma di coordinamento, in cui la partecipazione algoritmica prende il posto di istituzioni che pretendono il monopolio dell'autenticazione e della circolazione del valore [22, 11].

Questa formulazione è teoricamente rilevante anche per un'altra ragione. Essa impedisce di raccontare Bitcoin come se fosse solo l'effetto lineare di un'invenzione tecnica riuscita. Se si assume la tesi della soggettivazione collettiva, il protocollo appare invece come punto di incrocio tra etica condivisa, infrastruttura materiale e pratiche di cooperazione. La tecnica non viene prima e la politica dopo; al contrario, la politicizzazione è inscritta fin dall'inizio nella forma stessa che il protocollo assume e nella comunità che lo rende vivo [22].

Questa lettura consente anche di prendere sul serio il rapporto tra comunità ed evento tecnico. Il successo di Bitcoin nasce da un episodio di etica condivisa nel contesto di urgenti necessità di hackers su scala mondiale.

Questa formula è preziosa perché sottrae l'origine del protocollo alla mitologia dell'inventore isolato e la riconduce a un ecosistema di pratiche, aspettative e urgenze condivise. La comunità non viene dopo il protocollo come sua semplice utenza; ne costituisce piuttosto una condizione di possibilità storica.

Ne segue che la genealogia non va costruita come cronologia neutra di innovazioni. Va invece letta come processo in cui problemi tecnici e problemi politici si alimentano reciprocamente. Le mailing list, i primi fork, la scrittura del codice, le pratiche di manutenzione e la memoria del movimento fanno parte della storia di Bitcoin quanto l'algoritmo di consenso o la struttura del ledger. Trascurare questa dimensione significherebbe perdere proprio ciò che distingue il protocollo da una mera invenzione ingegneristica: il fatto di essere, fin dall'inizio, una forma di organizzazione del dissenso e della cooperazione [23].

In questa prospettiva Bitcoin può essere descritto anche come pratica di esodo. Il termine è utile se lo si intende con precisione: non come fantasia di uscita completa dai rapporti sociali esistenti, ma come tentativo di costruire spazi paralleli di validazione, circolazione del valore e cooperazione sottratti almeno in parte alle pratiche monetarie ufficiali e al monopolio degli intermediari. Ciò che qui conta non è importare integralmente una diagnosi esterna, ma riconoscere che la rottura inaugurata da Bitcoin si lascia leggere anche come sperimentazione di un'altra infrastruttura della fiducia [15].

Questa categoria aiuta inoltre a evitare una semplificazione ricorrente. L'emergenza di Bitcoin non va spiegata soltanto come effetto immediato della crisi del 2008, benché quella crisi ne abbia accelerato la visibilità e la legittimazione. Più radicalmente, l'esodo monetario che esso rende praticabile appartiene a una trasformazione di più lunga durata, legata alla digitalizzazione della produzione, della comunicazione e delle relazioni, dentro la quale si sono sedimentati saperi tecnici e desideri politici ostili alla finanziarizzazione e all'autorità monetaria centralizzata [15].

Il passaggio decisivo che politicizza questa traiettoria è il blocco finanziario a WikiLeaks. Quel momento mostra con chiarezza che i pagamenti non sono un semplice servizio neutrale, ma una infrastruttura politica capace di impedire o autorizzare l'esistenza materiale di soggetti, reti e pratiche di dissenso.

WikiLeaks non è l'origine assoluta di Bitcoin, ma il suo *καιρός*: non un semplice episodio cronologico, bensì il momento in cui una possibilità storica dispersa si condensa in evento costituente e diventa politicamente inaggirabile, nel senso proposto da Hardt e Negri [11]. Da quel momento risulta evidente che la neutralità del canale di transazione è una posta politica e non una caratteristica tecnica garantita una volta per tutte [21].

La Figura 1 sovrappone alla dinamica del primo mercato di Bitcoin una cronologia selettiva di eventi politici, mediatici, comunitari e tecnici. Il pannello superiore riporta il prezzo mediano in dollari registrato su Mt. Gox, la relativa banda mobile e i volumi giornalieri; il pannello inferiore rende visibili le oscillazioni percentuali, distinguendo quindi la direzione generale del prezzo dalla sua instabilità di breve periodo. Le linee e le annotazioni non identificano relazioni causali misurate, ma permettono di confrontare temporalmente eventi di natura diversa: il blocco finanziario a WikiLeaks tra la fine del 2010 e l'inizio del 2011; la prima esposizione su *Forbes* nel maggio 2011; le conferenze Bitcoin di Praga e Londra, che segnalano il consolidamento di una comunità pubblica; il furto di circa 43.000 bitcoin subito da Bitcoinica, che mostra invece la vulnerabilità degli intermediari sorti intorno al protocollo.

Il ruolo della figura nell'economia del testo è pertanto genealogico, non econometrico. Essa non dimostra che il blocco a WikiLeaks abbia determinato meccanicamente l'aumento del prezzo, ma mostra che la storia iniziale di Bitcoin non può essere letta attraverso la sola quotazione. Prima della visibilità finanziaria prodotta da *Forbes* e delle successive oscillazioni speculative, il grafico colloca un evento politico

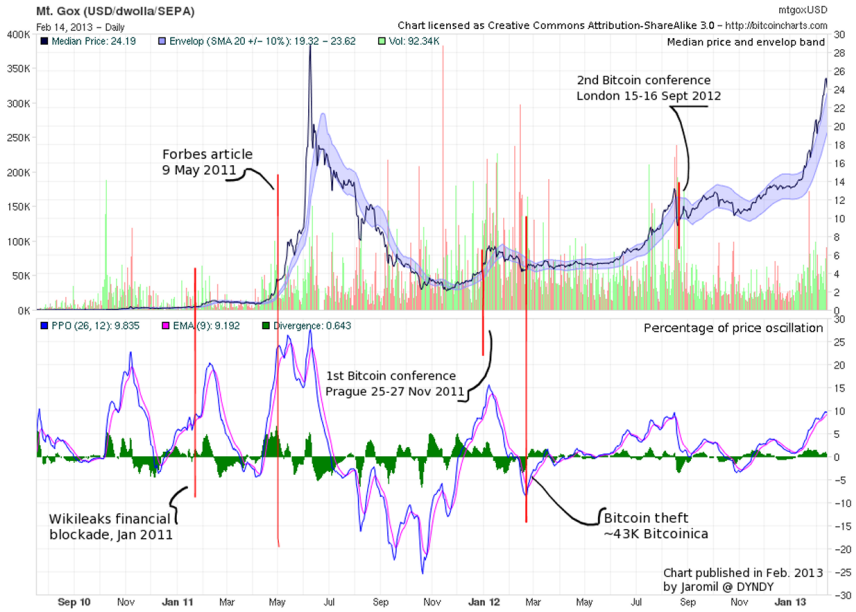


Fig. 1: Andamento del mercato Bitcoin su Mt. Gox tra il 2010 e il febbraio 2013, con alcuni eventi della sua prima storia pubblica. Il pannello superiore mostra il prezzo mediano in dollari, la banda mobile e i volumi di scambio; quello inferiore rappresenta l'oscillazione percentuale del prezzo. Le annotazioni collocano il blocco finanziario a WikiLeaks, l'articolo di *Forbes*, le conferenze di Praga e Londra e il furto subito da Bitcoinica. Fonte: elaborazione dell'autore su dati bitcoincharts.com, pubblicata nel febbraio 2013.

nel quale la non neutralità dei pagamenti diventa concretamente percepibile. Le conferenze documentano poi il passaggio dall'adozione dispersa alla formazione di uno spazio comunitario riconoscibile, mentre il caso Bitcoinica distingue la decentralizzazione del protocollo dalla fragilità delle piattaforme centralizzate che ne mediano l'uso. La figura condensa così, in forma visuale, i tre livelli che strutturano l'argomento dell'articolo: la crisi degli intermediari, la costituzione di una comunità e la successiva esposizione dell'infrastruttura alla finanziarizzazione e a nuove forme di intermediazione.

In questa sequenza il blocco finanziario a WikiLeaks precede la prima visibilità mainstream di Bitcoin e funziona da soglia di intelligibilità pubblica: l'infrastruttura monetaria smette di apparire come sfondo neutrale e si rivela come punto di applicazione del potere. In tal senso Bitcoin non arriva semplicemente *dopo* la crisi; ne assume l'urgenza come condizione di legittimazione storica. La domanda a cui risponde non è solo come trasferire valore digitalmente, ma come continuare a far circolare valore quando gli intermediari tradizionali si fanno dispositivi attivi di esclusione [23, 11].

L'importanza di WikiLeaks consiste proprio nel fatto che rende sensibile qualcosa che prima poteva restare implicito: il carattere selettivo e governamentale dell'infrastruttura monetaria. I circuiti di pagamento non si limitano a registrare scambi; selezionano, bloccano, gerarchizzano, rendono possibili alcune azioni e ne impediscono altre. In questo senso il caso WikiLeaks funziona come prova empirica di una tesi più ampia: la fiducia monetaria non è mai un puro fatto economico, ma sempre una costruzione politica e tecnica [16, 20].

Questa crisi della neutralità ha due effetti. Primo, rende visibile che il denaro è sempre già inscritto in dispositivi di governo. Secondo, spinge a cercare strumenti capaci di sottrarre la circolazione del valore al potere discrezionale di intermediari finanziari e regolativi.

In questa luce Bitcoin appare come risposta alla politicizzazione degli intermediari, non come fuga dalla politica. La sua novità consiste nell'aver mostrato praticamente che l'emissione, la verifica e il trasferimento di valore possono essere ricombinati in una architettura distribuita [21].

Per questo motivo la rottura del taboo del denaro non va intesa come semplice desacralizzazione ideologica. Essa è una dimostrazione pratica di alternative sistemiche. Ciò che si rompe non è soltanto una credenza culturale, ma un regime di impensabilità: l'idea che la moneta non possa essere oggetto di sperimentazione dal basso, che il suo disegno appartenga solo a istituzioni sovrane o a apparati finanziari consolidati. Nel momento in cui Bitcoin mostra che il denaro può essere reimmaginato come infrastruttura condivisa, apre anche la possibilità di nuove sovranità costituenti [21, 23].

Da qui deriva anche il carattere non puramente reattivo di Bitcoin. Sebbene il protocollo nasca in un contesto segnato da crisi e censura, il suo significato non si esaurisce nella difesa.

Bitcoin non è solo riparo dalla chiusura dei canali; è anche apertura di uno spazio positivo di sperimentazione istituzionale. Questo aspetto è fondamentale: ciò che il protocollo inaugura non è solo una tecnica di resistenza, ma anche un laboratorio di nuove forme di razionalità, di nuove regole e di nuove possibilità di cooperazione [23].

La rottura del taboo del denaro consiste esattamente in questo. Ciò che per secoli era apparso come una funzione non contendibile viene sottoposto a redesign. La moneta diventa oggetto di sperimentazione infrastrutturale. Una simile rottura non dissolve il problema della sovranità, ma lo riapre. La domanda cessa di essere chi possieda legittimamente il monopolio del denaro e diventa piuttosto come tale funzione possa essere redistribuita, autenticata e governata attraverso il protocollo.

Da questo punto di vista la genealogia non serve a costruire un mito delle origini, ma a chiarire la natura del conflitto inaugurato da Bitcoin. Se il protocollo emerge all'incrocio tra etica condivisa, crisi degli intermediari e sperimentazione infrastrutturale, allora il suo senso storico non può essere ridotto né all'apologetica finanziaria né alla demonizzazione morale. Va piuttosto compreso come punto di biforcazione: il momento in cui il denaro smette di essere un tabù e diventa il primo terreno di prova di una più ampia politica delle infrastrutture programmabili [22].

3 Bitcoin come infrastruttura politico-tecnica

La forza di Bitcoin sta nell'aver trasformato la critica degli intermediari in una infrastruttura operativa. Il mining redistribuisce l'autenticazione monetaria; il ledger condiviso istituisce un registro resistente alla manipolazione; il protocollo salda regola, incentivo e verifica in una forma coerente. In questo senso Bitcoin non è semplicemente una moneta digitale, ma una infrastruttura di autenticazione e contabilità che ricodifica il rapporto tra fiducia e partecipazione [21, 10].

Una formula particolarmente efficace descrive il passaggio così: una moltitudine distribuita sostituisce il monopolio della violenza con la partecipazione algoritmica.

Anche se tale formula va maneggiata criticamente, essa coglie un punto decisivo. Con Bitcoin la garanzia della transazione non è più affidata a un centro sovrano unico, ma a un dispositivo in cui i partecipanti stessi concorrono alla validazione. Il corpo sociale si fa garante dell'autenticazione transazionale, sia pure entro regole rigidamente codificate.

Qui diventa utile introdurre una delle obiezioni più note contro il mining: Bitcoin sarebbe una "Rube Goldberg machine" per comprare elettricità [21, 5]. L'espressione indica un congegno deliberatamente complicato che impiega una lunga catena di

operazioni per ottenere un risultato semplice. Applicata a Bitcoin, la metafora presenta il proof of work come una procedura inutilmente dispendiosa: milioni di operazioni di hashing verrebbero eseguite soltanto per produrre una scarsità artificiale che potrebbe essere definita direttamente mediante una formula. Nella formulazione originaria della critica, sarebbe sufficiente stabilire nel tempo un limite all'emissione, mantenere pubbliche le transazioni e verificarle mediante firme crittografiche, senza trasformare continuamente elettricità in tentativi computazionali.

La critica coglie un aspetto reale: il lavoro dei miners non produce un bene esterno alla rete e, considerato isolatamente, appare come una ricerca ripetitiva di numeri. La mia risposta consiste però nel rifiutare proprio questo isolamento concettuale. Il mining non svolge soltanto la funzione di emissione monetaria; il medesimo lavoro concorre a ordinare le transazioni, rendere costosa la riscrittura del registro e rafforzare l'autenticazione condivisa. Il consumo di energia non è quindi un passaggio aggiunto dopo la creazione della moneta, ma parte del dispositivo con cui la rete costruisce fiducia nella propria storia contabile.

Anche il termine di paragone deve essere reso esplicito. L'alternativa storica non è una autenticazione monetaria priva di costi materiali, bensì la zecca tradizionale: procedure riservate di conio, grandi macchinari, edifici protetti e guardie armate. Bitcoin non elimina l'energia necessaria a istituire e difendere l'autenticità della valuta; la ricodifica. A una energia concentrata e gerarchicamente custodita sostituisce una energia computazionale distribuita tra peers. Il network dei miners opera così come una zecca condivisa, una "clusterizzazione della zecca" nella quale la protezione dell'autenticità non dipende da un perimetro armato, ma dalla cooperazione competitiva dei nodi [21].

In questo senso la formula secondo cui "la partecipazione ha sostituito la violenza nell'adempimento fisico dell'autenticazione della valuta" descrive una trasformazione istituzionale, non l'assenza di costi o conflitti. La funzione di garanzia viene trasferita da un apparato sovrano che concentra autorizzazione, emissione e coercizione a una procedura infrastrutturale aperta alla partecipazione. Questa risposta non dimostra che ogni livello di consumo energetico sia giustificato, né risolve il problema della redistribuzione della ricchezza prodotta dal mining. Mostra piuttosto perché il proof of work non possa essere valutato come puro dispendio entropico: il suo costo va discusso in rapporto alla funzione di autenticazione e all'assetto politico-materiale che sostituisce.

Anche per questo il ledger distribuito va sottratto alla retorica che lo descrive come semplice contenitore neutrale. Va compreso più precisamente come innovazione contabile, o addirittura come forma di triple-entry accounting, in cui la registrazione condivisa e verificabile della transazione si aggiunge alle due scritture delle parti. Questa formulazione è importante perché sposta lo sguardo dal feticcio della "catena" al regime di registrazione che essa rende possibile. Prima che una metafisica della decentralizzazione, esso è una tecnica di contabilità condivisa, cioè un modo specifico di organizzare memoria, sequenza, prova e verificabilità [10, 17, 16].

Da qui emerge la centralità della sovranità algoritmica. La sovranità non scompare, ma cambia sede. Una parte della funzione sovrana viene incorporata nel protocollo, nei criteri di validazione, negli incentivi economici e nella materialità dell'infrastruttura.

Parlare di sovranità algoritmica significa allora chiedersi in quali condizioni autenticazione, decisione e coordinamento siano organizzati da regole tecniche che pretendono di valere in modo impersonale. Significa anche chiedersi chi progetta tali regole, chi può modificarle, chi può comprenderle e chi ne sopporta i costi [22, 25].

Su questo punto il riferimento ai "Bitcoin Improvement Proposals" (BIP) è particolarmente istruttivo. Se Bitcoin può essere descritto come meccanismo di proposte, discussioni, implementazioni e biforcazioni, allora la sovranità algoritmica non coincide con un automatismo cieco del codice. Essa si manifesta invece nell'intreccio tra forma protocollo e processi comunitari di negoziazione tecnica. Il protocollo pretende impersonale necessità, ma vive di comunità, manutenzione, conflitto e decisioni stratificate. La sua sovranità è dunque sempre contemporaneamente tecnica e sociale.

Questo spostamento non autorizza alcuna mitologia della neutralità. Un registro distribuito non è mai un supporto tecnico indifferente. Esso distribuisce accessi, visibilità, tempi di validazione, costi di partecipazione e poteri di intervento in modo differenziale. Perciò la network neutrality va pensata qui anzitutto come tema storicamente specifico delle infrastrutture di rete: l'idea che il canale debba restare il più possibile indiscriminato, non selettivo rispetto ai contenuti, agli attori e agli usi, così da rendere praticabile una partecipazione senza censura preventiva.

La sua importanza, anche per Bitcoin, è evidente. Senza un qualche grado di neutralità infrastrutturale, la promessa anti-censura della rete si svuota rapidamente, perché i punti di accesso, instradamento o pagamento possono essere piegati a funzioni di filtraggio, esclusione e comando. Proprio per questo la neutralità della rete ha funzionato per lungo tempo come utopia trasversale: un orizzonte condiviso, pur con motivazioni diverse, da culture hacker, attivisti, tecnici, operatori del software libero e difensori delle libertà civili.

Ma la sua forza normativa non deve far dimenticare la sua parziale infattibilità. Una neutralità piena e definitiva delle infrastrutture è difficilmente raggiungibile, se non impossibile, perché ogni rete concreta incorpora gerarchie materiali, colli di bottiglia, regole di priorità, regimi di visibilità e poteri di interdizione. In questo senso la network neutrality non va assunta come stato puro da presupporre, bensì come problema politico-istituzionale permanente: non solo assenza di censura sul canale, ma conflitto continuo su chi controlla le condizioni materiali di accesso, trasferimento e validazione. La promessa originaria anti-censura di Bitcoin resta importante, ma va sottratta a ogni lettura ingenua [4, 1].

La decentralizzazione stessa, da questo punto di vista, resta concetto irriducibilmente ambiguo. Come nota Brekke, essa oscilla tra una maggiore autonomia per i partecipanti e la consegna del controllo ad architetture algoritmiche distribuite che possono risultare tanto difficili da contestare quanto i vecchi centri di comando. Si può parlare qui anche di un vero e proprio feticismo della rete: la tendenza a proiettare sulla forma distribuita dell'infrastruttura qualità normative come libertà, neutralità o democrazia, occultando le relazioni di potere, le dipendenze materiali e le asimmetrie che continuano a strutturarla [2].

Una topologia decentralizzata può certamente rendere più difficile la censura diretta e l'arresto dell'intera rete, ma non garantisce da sola esiti egualitari o democratici. Il protocollo distribuisce il potere; non per questo lo distribuisce simmetricamente [4].

Qui entra in gioco anche il tema del minimalismo. La crescita di dipendenze, stratificazioni e complessità del software indebolisce la promessa di autonomia. Se una città intera non può comprendere la quantità di dipendenze che sorreggono un'infrastruttura, allora l'indipendenza dagli intermediari giuridici o bancari rischia di essere compensata da una nuova eteronomia tecnica. Per questo la sovranità algoritmica non va misurata solo dalla resistenza alla censura, ma anche dalla possibilità concreta di capire e governare il sistema [22].

Il minimalismo non è allora una virtù meramente stilistica, ma una condizione di sicurezza. Più un protocollo accumula livelli opachi, librerie non auditabili e astrazioni superflue, più aumenta la sua superficie d'attacco e più si restringe il numero di soggetti in grado di verificarne davvero il funzionamento. Un'infrastruttura può anche essere formalmente open source e restare, nei fatti, inaccessibile alla revisione pubblica: in quel caso la sicurezza tende a dipendere da specialisti, manutentori e cerchie ristrette, cioè da nuove forme di intermediazione tecnica.

Il punto decisivo è che leggibilità, auditabilità e semplicità relativa del design hanno effetti immediatamente politici. Rendono più facile condividere saperi, distribuire capacità di intervento, formare nuovi manutentori e ridurre l'asimmetria tra chi usa il sistema e chi può modificarlo. In questo senso il minimalismo funziona come condizione materiale della partecipazione: non garantisce da solo esiti democratici, ma rende più plausibile che il controllo sull'infrastruttura non si concentri in una casta tecnica.

Vale anche il contrario. Quando il protocollo diventa troppo complesso per essere compreso, discusso o riprodotto senza una lunga catena di deleghe, la distribuzione formale del consenso convive con una concentrazione sostanziale del sapere e quindi del potere. La condivisione delle regole si rovescia in dipendenza dai loro interpreti privilegiati. Per questo il minimalismo va trattato come criterio insieme epistemico, securitario e politico: ridurre il superfluo significa non solo diminuire il rischio tecnico, ma anche allargare la base sociale della verifica, del dissenso e della manutenzione [22]. La conseguenza più importante di questa impostazione è che Bitcoin non elimina la

politica: la ricodifica. Il conflitto non scompare, ma si sposta. Si sposta sul design del protocollo, sui costi energetici e materiali del consenso, sulle forme di centralizzazione del mining, sulle soglie di ingresso e sulle modalità con cui una comunità può riconoscersi o fratturarsi intorno alle sue regole. Da questo punto di vista Bitcoin va letto come un dispositivo tecnico-politico che ha reso visibile una nuova sede della sovranità, senza per questo risolverne automaticamente le contraddizioni, ma aprendo il campo a nuove possibilita' di soluzione o problematizzazione. È Un dispositivo che ci proietta su un campo più ampio, inclusivo ed interdisciplinare, e che oserei definire più scientifico, organizzabile, trasparente e razionale di quello offertoci dalle teorie di macro-economia moderna e dalle infrastrutture finanziarie del ventesimo secolo. Per quanto possa sembrare caotico, soprattutto a causa dell'improvvisa inclusività di realtà liminali ed al confine con la criminalità nel suo momento di genesi, questo dispositivo ci apre dei processi progettuali sempre più governabili, istituzionalizzabili ed appropriabili al contesto.

4 Dal protocollo alla governance: espansione, ambivalenza, conflitto

Dal nucleo monetario di Bitcoin si sviluppa progressivamente un più ampio insieme di piattaforme, protocolli e ambienti di esecuzione. Con smart contract, DAO e stack applicativi derivati, il problema smette di riguardare solo il trasferimento di valore e investe la governance, il diritto, la coordinazione collettiva e l'architettura delle applicazioni.

Questa espansione non va letta come semplice crescita lineare dell'innovazione, ma come effetto della rottura inaugurale di Bitcoin: una volta infranto il taboo del denaro, diventa pensabile riorganizzare come infrastrutture programmabili anche altre funzioni sociali [23]. La questione che tiene insieme i fenomeni discussi in questa sezione è dunque la seguente: che cosa accade quando la programmabilità si estende dalla transazione monetaria alle condizioni tecniche della cooperazione?

4.1 Programmare la governance

Il passaggio tecnico decisivo è rappresentato dall'ascesa di Ethereum e dei suoi smart contract. Uno smart contract è anzitutto un binario eseguibile in modo deterministico su una rete di calcolo decentralizzata: a parità di input, produce gli stessi output. La sua importanza teorica non risiede quindi in una presunta "intelligenza", ma nel trasferimento del rapporto contrattuale sul terreno della computazione verificabile e dei suoi vincoli [23].

Il determinismo che rende possibile l'esecuzione distribuita impone però una riduzione della complessità sociale. Ciò che può essere formalizzato entra nel protocollo; il resto viene approssimato, espulso o trasferito altrove. Ogni volta che

un problema politico viene codificato in forma eseguibile si decide, pertanto, quali aspetti della relazione collettiva siano resi computabili e quali restino fuori campo [23, 12]. L'espansione dal denaro alla governance non elimina il conflitto: lo anticipa nel disegno delle categorie, delle procedure e degli input ammessi dal sistema.

Le DAO rendono visibile questa tensione. Promettono coordinamento distribuito e governance senza centro, ma nella pratica dipendono spesso da ambienti centralizzati, competenze specialistiche e meccanismi di voto che trasformano la partecipazione in pesatura patrimoniale. La tecnologia non ha risolto le difficoltà proprie di modelli di governance grandi, distribuiti e culturalmente eterogenei. La DAO va quindi considerata un laboratorio, non una soluzione: mostra il tentativo di fare della governance un problema di design infrastrutturale e, nello stesso tempo, il limite di una riduzione del politico al tecnico. Nella sua formulazione più forte, l'on-chain governance comprime infatti interpretazione, mediazione e conflitto entro procedure computabili [23].

La decentralizzazione non coincide dunque con la democratizzazione. Può ridurre alcuni arbitrii, ma può anche produrre nuove elite tecniche, dipendenze infrastrutturali e forme di plutocrazia. Per valutarne gli effetti occorre osservare non soltanto il protocollo, ma l'intero stack che rende possibile la partecipazione.

4.2 Infrastruttura, privacy e usi concreti

La nozione di "web3", intesa come stack applicativo, consente di descrivere questo insieme come combinazione di rete peer-to-peer, algoritmo di consenso, macchina virtuale e libro mastro immutabile. Tale descrizione architetturale sottrae il campo alla retorica promozionale e permette di individuare dipendenze tecniche, gerarchie di accesso e condizioni di verificabilità nei diversi livelli dell'infrastruttura [23].

Le operazioni svolte restano relativamente sobrie: registrare stati e transazioni in forma condivisa, eseguire script deterministici, coordinare accessi, firme, proprietà, votazioni, scambi e incentivi. La loro portata politica deriva non da una qualità intrinsecamente "smart" o "decentralizzata", ma dall'assemblaggio di algoritmi, dati, macchine, regole di accesso e pratiche d'uso. Le piattaforme derivate non rappresentano quindi una semplice estensione tecnica di Bitcoin: intensificano una razionalità infrastrutturale che investe automazione, coordinamento e cattura del valore [23, 29]. Per questo il lessico valoriale di democrazia, libertà e partecipazione non può sostituire criteri di giudizio tecnopolitico, soprattutto in un campo segnato da una forte crescita degli investimenti.

La prima condizione politica da verificare è la privacy dei partecipanti. Essa non può essere ridotta alla segretezza dei contenuti, ma deve comprendere l'anonimato di rete, affinchè la partecipazione non divenga una trappola di controllo [18]. L'anonimato non è semplice occultamento identitario: sottrae relazioni, pratiche e cooperazione all'obbligo di convertirsi in profili e valore estraibile, custodendo uno

spazio di azione collettiva non immediatamente catturato da sorveglianza, intelligence e valorizzazione algoritmica [24]. Il progetto "web3privacy now", sviluppato entro l'ambiente Ethereum e web3, esprime questa consapevolezza quando presenta la privacy come condizione di autonomia, dignità e autodeterminazione, non come sola protezione dei dati personali [19].

La verificabilità di una infrastruttura condivisa può infatti convivere con l'esposizione permanente dei soggetti. Se ogni interazione può essere tracciata, correlata o impiegata per costruire profili di rischio, il protocollo assume una funzione panottica [18, 7, 1]. Senza anonimato, la comunicazione stessa tende a diventare occasione di sorveglianza e cattura, restringendo la possibilità di usi autonomi delle infrastrutture comuni [24].

L'ambivalenza diventa concreta negli impieghi industriali e territoriali. I regimi di predizione rendono il futuro calcolabile per intervenire sul presente: dati su consumi, spostamenti e comportamenti possono riallineare produzione, distribuzione e trasporto, mentre sensori e protocolli intelligenti adattano le decisioni operative a pattern di uso e consumo [7, 22]. La stessa capacità infrastrutturale può dunque migliorare il coordinamento dei flussi o ampliare la profilazione e il controllo.

In questo quadro le monete complementari non sono esempi ornamentali, ma dispositivi capaci di coordinare incentivi, clearing e ricompense in ecosistemi territoriali nei quali trasporto, prossimità e cooperazione materiale sono centrali. L'interconnessione tra valute, gli incontri peer-to-peer e l'ottimizzazione dei trasporti su scala municipale mostrano che il problema non riguarda soltanto il pagamento, ma l'organizzazione dei flussi e la loro governabilità tecnica [22, 21]. Questi esperimenti investono insieme moneta, cooperazione sociale, assetti istituzionali e resilienza territoriale [9]. Proprio per questo restano ambivalenti: possono sostenere mutualismo e coordinamento locale, ma anche intensificare sorveglianza, selezione e modulazione dei comportamenti.

Il settore nucleare offre un secondo esempio, diverso ma complementare. Nelle procedure di safeguards, il valore delle tecnologie derivate da Bitcoin non risiede in una generica promessa di innovazione, bensì in funzioni circoscritte e verificabili: immutabilità pratica nella gestione delle identità dei sensori, timestamping decentralizzato per provare esistenza e inalterazione dei dati, audit trail per ridurre errori clericali e controversie sulla responsabilità [28]. Questo caso mostra che la valutazione tecnopolitica deve partire dalle funzioni effettive, dagli attori che possono verificarle e dalle responsabilità che l'infrastruttura rende visibili o opache.

4.3 Leggibilità, diritto e alternative

La possibilità di verificare queste funzioni introduce il problema della leggibilità. Gli intermediari non spariscono: cambiano forma. Al posto del banchiere o del funzionario possono comparire il manutentore invisibile del protocollo, il progettista degli incentivi e l'esperto che controlla la complessità. La leggibilità del codice e la

discussione pubblica delle regole sono quindi condizioni politiche della partecipazione [22].

L'opacità riguarda l'intero assemblaggio operativo: infrastrutture di calcolo, dati, interfacce, automatismi decisionali e dipendenze tecniche. La disponibilità del codice sorgente non basta se i partecipanti non possono comprendere come l'automazione si innesti nella cooperazione sociale [29]. Acquistano perciò rilievo i tentativi di esprimere i contratti in linguaggi di alto livello accessibili anche a non specialisti. Zenroom e Zencode, impiegati anche nel contesto applicativo nucleare, formulano smart contract in un linguaggio leggibile dagli umani, avvicinando l'esecuzione tecnica alla discussione pubblica delle regole [28, 6].

La domanda discriminante diventa allora se si stiano sviluppando tecnologie perché le macchine percepiscano le persone oppure perché le persone possano comprendere le macchine. Nel primo caso la rete tende verso profilazione e opacità decisionale; nel secondo la tecnica può diventare oggetto di apprendimento, discussione e autodeterminazione collettiva. La consapevolezza non è una virtù pedagogica accessoria, ma un criterio politico di progettazione.

Questo criterio conduce alla normatività incorporata nel codice. Una regola automatizzabile non è per ciò stesso giusta, contestabile o politicamente legittima. Le infrastrutture programmabili non sostituiscono il problema del diritto, ma lo redistribuiscono tra design del protocollo, soglie di accesso, meccanismi di aggiornamento e regimi di visibilità [26, 27].

La tensione tra "rule of law" e "rule of code" porta questo problema alla sua formulazione più radicale. I sistemi basati su registri distribuiti e macchine virtuali imitano l'impersonalità della legge mediante l'esecuzione tecnica della regola, ma entrano in conflitto con il diritto quando eliminano interpretazione, contestazione e revisione pubblica. Non si tratta di scegliere tra codice e diritto come sfere separate: il protocollo è uno dei luoghi in cui vengono redistribuite autorità, neutralità e possibilità di intervento [26, 27].

L'esito dell'espansione dal protocollo alla governance resta pertanto aperto. Le stesse infrastrutture possono rendere praticabili beni comuni digitali, monete complementari, modelli cooperativi e forme di coordinamento non subordinate ai centri tradizionali; possono però anche favorire sorveglianza, finanziarizzazione, cattura corporativa e concentrazione plutocratica del consenso. La nozione di tendenza autocratica nomina questo possibile rovesciamento della promessa iniziale di democratizzazione. Le alternative non risiedono in una proprietà automatica della tecnologia, ma in pratiche orientate ai beni comuni, tooling per attivisti, modelli cooperativi, mutualismo infrastrutturale e infrastrutture resilienti. La sfida consiste nel progettare e governare questi dispositivi senza tradirne integralmente l'impulso costituente [4].

5 Conclusione

Bitcoin resta una rottura storica perché ha mostrato che denaro, fiducia e coordinamento possono essere ripensati come problemi infrastrutturali.

In questo gesto il protocollo ha aperto una nuova fase di sperimentazione storica, in cui una parte delle funzioni tradizionalmente attribuite alla sovranità viene ricodificata in regole tecniche, incentivi economici e partecipazione distribuita. Tale spostamento non ha abolito la politica, come spesso accade nel caso di piattaforme proprietarie; l'ha resa nuovamente visibile nel punto in cui codice, comunità e infrastruttura si incontrano [22].

L'analisi genealogica proposta qui consente di chiarire che la sovranità algoritmica non è un fondamento puro. È un terreno di conflitto.

Bitcoin nasce come risposta alla politicizzazione degli intermediari e alla crisi della neutralità delle infrastrutture di pagamento, ma la sua traiettoria successiva mostra quanto facilmente una promessa di autodeterminazione possa essere assorbita da logiche di finanziarizzazione, centralizzazione e comando tecnico. La decentralizzazione non basta a garantire esiti democratici, così come l'apertura formale del codice come "software libero ed open source" non basta a produrre consapevolezza collettiva [4].

La ricostruzione svolta nelle sezioni precedenti suggerisce anche una conseguenza metodologica. Non basta analizzare i protocolli come oggetti tecnici, così come non basta ricondurli a semplici effetti di ideologie economiche esterne. Occorre invece seguirne la composizione concreta: pratiche comunitarie, dispositivi di validazione, regimi di visibilità, incentivi, dipendenze software, soglie di accesso e processi di aggiornamento. Solo una simile analisi consente di capire in che senso la sovranità algoritmica sia insieme una promessa di autodeterminazione e una possibile forma di cattura [7, 12, 16].

Questa impostazione implica anche un cambiamento di scala analitica: non basta chiedersi se una singola tecnologia sia o no decentralizzata. Occorre chiedersi quali concatenamenti istituzionali, economici e culturali essa renda stabili, quali forme di soggettività produca, quali comportamenti incentivi e quali orizzonti di azione chiuda o apra. In tal senso, questo campo va trattato come ambiente storico più che come insieme di strumenti isolati: un ambiente in cui il problema del governo attraversa insieme codice, infrastruttura, comunità, diritto e immaginario [7, 1, 27].

In questo quadro, la questione della privacy e quella della consapevolezza acquistano un ruolo strategico. Se la partecipazione avviene in ambienti che espongono integralmente i soggetti oppure restano illeggibili ai più, la promessa di disintermediazione si rovescia rapidamente in una nuova tecnocrazia.

Allo stesso modo, se la neutralità della rete viene trattata come dato naturale e non come problema istituzionale, diventa impossibile vedere chi controlla davvero le condizioni di accesso, trasferimento e validazione. La critica di queste infrastrutture non può perciò limitarsi a denunciare gli esiti peggiori: deve studiare le condizioni materiali che li rendono probabili attraverso la lente di analisi della tecno-politica [18, 14].

Questa attenzione alle condizioni materiali permette anche di riformulare in modo più preciso il problema democratico. Il nodo non è soltanto chi possieda l'infrastruttura, ma chi possa comprenderla, contestarla e modificarla. Una rete formalmente aperta ma praticamente incomprensibile replica, sotto altra forma, il vecchio problema dell'opacità istituzionale. Da questo punto di vista, leggibilità del codice, tooling democratico e pratiche cooperative non sono elementi accessori o idealistici: sono condizioni di possibilità di qualsiasi effettiva redistribuzione del potere [22].

Se questa diagnosi è corretta, il compito teorico e politico successivo non consiste né nell'apologia né nella demonizzazione di Bitcoin o delle infrastrutture che ne sono o saranno derivate. Consiste piuttosto nel contendere le implicazioni politiche della tecnologia: neutralità dei canali, privacy effettiva, leggibilità delle regole, possibilità di contestazione, design orientato ai valori e istituzioni cooperative. Il punto non è difendere astrattamente un'origine presunta pura, ma lavorare sulle condizioni in cui Bitcoin e le tecnologie da esso derivate possano ancora essere piegate verso forme di coordinamento meno plutocratiche e più democratiche. Se il loro potenziale trasformativo non vuole esaurirsi nella sola dimensione speculativa, esso richiede infatti un processo di istituzionalizzazione capace di articolare design monetario, governance, regole di accesso e finalità pubbliche [8].

Ciò significa anche riconoscere che le alternative democratiche non nascono fuori dal campo, come semplice rifiuto morale del protocollo.

Nascono piuttosto all'interno delle sue contraddizioni: come sperimentazioni cooperative, come interventi sul design e come conflitti sulla governance. Se Bitcoin ha aperto il denaro alla progettazione, il compito successivo è aprire la progettazione stessa alla deliberazione, alla critica e alla partecipazione dei soggetti che dovranno abitarne gli effetti.

Una simile traiettoria propositiva può essere intravista anche in sperimentazioni territoriali che ridimensionano la moneta alla sua funzione e spostano l'attenzione sull'infrastruttura che la rende operabile. Il caso di Lugano, con l'ecosistema My-Lugano/LVGA sviluppato nel contesto del Lugano Living Lab e oggi sostenuto anche dalla Fondazione PlanB, mostra che un token locale può valere non come novità monetaria in sé, ma come componente di una più ampia infrastruttura urbana di incentivo economico e coordinamento economico, supporto all'adozione e governance amministrata. In questo senso, la posta politica non risiede nell'enfasi sulla moneta,

ma nella possibilità di costruire piattaforme civiche leggibili, istituzionalmente responsabili e capaci di orientare strumenti digitali verso finalità pubbliche e territoriali [3].

In questo senso il contributo di Bitcoin non si esaurisce nella propria traiettoria storica. Esso lascia aperto un problema costituente: come organizzare infrastrutture condivise che non dipendano integralmente né dal monopolio degli intermediari tradizionali né da nuove oligarchie tecniche e patrimoniali. È nei luoghi e tempi in cui questi conflitti si palesano e si affrontano in modo consapevole che la sovranità algoritmica può diventare il terreno di una effettiva autodeterminazione sociale.

Biografia dell'Autore. Denis Roio, noto anche come Jaromil, svolge attività di ricerca e sviluppo nell'ambito del software libero, della crittografia applicata, delle infrastrutture decentralizzate e della sovranità algoritmica. È direttore scientifico della Fondazione PlanB a Lugano.

Dichiarazione. L'autore dichiara il proprio coinvolgimento professionale nella traiettoria discussa nel caso di Lugano, in qualità di direttore scientifico della Fondazione PlanB. Il caso MyLugano/LVGA è presentato come banco di prova per valutare la leggibilità sociale, l'orientabilità democratica e la sostenibilità istituzionale di infrastrutture civiche digitali, non come eccezione da celebrare.

References

1. Claudia Aradau and Tobias Blanke. Politics of prediction: Security and the time/space of governmentality in the age of big data. *European Journal of Social Theory*, 20(3):373–391, 2017.
2. Jon Baldwin. In digital we trust: Bitcoin discourse, digital currencies, and decentralized network fetishism. *Palgrave Communications*, 4(1), 2018.
3. Lorenzo Barisone, Edoardo Beretta, Robert Bregy, Vincenzo Carbone, Roberto Gorini, and Giacomo Zucco. Blockchain adoption in local governments: The case of lugano. *FinTech*, 5(1):24, 2026.
4. Jan Arild Brekke. Hacker-engineers and their economies: The political economy of decentralised networks and 'cryptoeconomics'. *New Political Economy*, 2020.
5. Niccolo Caldararo. Bitcoin: Rube goldberg machine, antique throwback, gigantic distraction, entertainment, ripoff or new money? *Interdisciplinary Description of Complex Systems: INDECS*, 16(3-B):427–445, 2018.
6. A D'Intino and D Roio. Smart contracts for data commons integrated with gdpr compliant legal rules: Zencode, 2023.
7. Simon Egbert. Algorithmic futures: Governmentality and prediction regimes. In *Algorithmic Regimes: Methods, Interactions, and Politics*, pages 265–285. Amsterdam University Press, Amsterdam, 2024.
8. Marco Fama and Stefano Lucarelli. Una politica economica per le criptovalute. *Moneta e Credito*, 78(309):27, 2025.

9. Marco Fama, Stefano Lucarelli, Ricardo Orzi, et al. Rethinking money, rebuilding communities. a multidimensional analysis of crypto and complementary currencies. *Partecipazione e conflitto*, 13(1-Special Issue 2):337–359, 2020.
10. Ian Grigg. Triple entry accounting. *Journal of Risk and Financial Management*, 17(2):76, 2024.
11. Michael Hardt and Antonio Negri. *Commonwealth*. Harvard University Press, 2009.
12. Lucas Introna. Algorithms, governance, and governmentality: On governing academic writing. *Science, Technology, & Human Values*, 41(1):17–49, 2016.
13. Colin Koopman. *Genealogy as critique: Foucault and the problems of modernity*. Indiana University Press, 2013.
14. Susanne Krasmann. The logic of the surface: On the epistemology of algorithms in times of big data. *Information, Communication & Society*, 23(14):2096–2109, 2020.
15. Christian Marazzi. La violenza del capitalismo finanziario. *Crisi dell'economia globale. Mercati finanziari, lotte sociali e nuovi scenari politici*, pages 17–49, 2009.
16. Peter Miller. Governing by numbers: Why calculative practices matter. *Social Research*, 68(2):379–396, 2001.
17. Peter Miller and Ted O'Leary. Governing the calculable person. In Anthony G. Hopwood and Peter Miller, editors, *Accounting as Social and Institutional Practice*, pages 98–115. Cambridge University Press, Cambridge, 1994.
18. Rainer Muhlhoff. Predictive privacy: Towards an applied ethics of data analytics. *Ethics and Information Technology*, 23(4):675–690, 2021.
19. PG. From cypherpunk to carepunk. *Web3Privacy*, 2024. Position paper, accessed 18 March 2026.
20. Theodore M. Porter. *Trust in Numbers: The Pursuit of Objectivity in Science and Public Life*. Princeton University Press, Princeton, 1995.
21. Denis Roio. Bitcoin: La fine del tabu della moneta. Effimera, 2014.
22. Denis Roio. *Algorithmic Sovereignty*. PhD thesis, University of Plymouth, 2018. PhD thesis.
23. Denis Roio. Il vero movimento crypto. Makery, Italian version of "From Commons to NFTs", 2022.
24. Ned Rossiter and Soenke Zehle. Toward a politics of anonymity. *The Routledge Companion to Alternative Organization*, 2014.
25. Antoinette Rouvroy. Technology, virtuality and utopia: Governmentality in an age of autonomic computing. In Mireille Hildebrandt and Antoinette Rouvroy, editors, *Law, Human Agency and Autonomic Computing*, pages 119–140. Routledge, London, 2011.
26. Antoinette Rouvroy. The end(s) of critique: Data behaviourism versus due process. In Mireille Hildebrandt and Katja de Vries, editors, *Privacy, Due Process and the Computational Turn: The Philosophy of Law Meets the Philosophy of Technology*, pages 143–167. Routledge, London, 2013.
27. Antoinette Rouvroy and Bernard Stiegler. The digital regime of truth: From the algorithmic governmentality to a new rule of law. *La Deleuziana*, 3:6–27, 2016.
28. Marco Sachy, Roberto Spigolon, and Stefan Nonneman. Three properties of distributed ledger technology systems applied in the nuclear sector adding value to safeguards—immutability, timestamping and auditability. *IJNSNP*, 62:60–79, 2021.
29. Tiziana Terranova. *After the internet: Digital networks between capital and the common*, volume 33. MIT Press, 2022.

Scalare Bitcoin oltre la Timechain

Gianluca Cappiello

BitPolito, Politecnico di Torino, Italy

Abstract. La scalabilità rappresenta il limite strutturale di Bitcoin, derivante dal principale problema della sua timechain: un basso throughput causato dalle restrizioni su dimensione e frequenza dei blocchi. Questo contributo analizza le ottimizzazioni on-chain (Layer 1) implementate nel protocollo, come SegWit, volte a rendere più efficiente l'uso dello spazio nel blocco e a incrementare la capacità della rete. Nonostante tali sforzi, la scalabilità di massa richiede un cambio di paradigma. Vari protocolli, fungendo da Layer 2, offrono una risposta al problema permettendo l'esecuzione off-chain di transazioni istantanee e a basso costo, spostando dunque l'onere dal Layer 1 e realizzando il potenziale di Bitcoin per un uso quotidiano.

Keywords: Scalabilità · Soft Fork · Layer 2

1 Introduzione

Il protocollo Bitcoin, introdotto da Satoshi Nakamoto nel 2008 [14], risolve il problema del *double-spending* in un sistema distribuito attraverso il meccanismo di consenso Proof-of-Work (PoW), senza ricorrere ad alcuna autorità centrale.
Le scelte progettuali volte a massimizzare decentralizzazione e sicurezza impongono però vincoli stringenti sulle prestazioni, rendendo la scalabilità il principale punto critico del protocollo.

1.1 Primitive Crittografiche

Bitcoin sostituisce l'intermediario centralizzato nello scambio di valore con un sistema crittografico distribuito. Grazie alla crittografia a curve ellittiche (ECC) e alle firme digitali, gli utenti possono dimostrare la proprietà dei fondi e autorizzare transazioni senza affidarsi a terze parti.

De Cifris Koine – BITCOIN & BLOCKCHAIN
https://doi.org/10.69091/koine/vol-6-B03

Crittografia a Curve Ellittiche (ECC). Bitcoin utilizza la curva `secp256k1` definita sul campo finito $\mathbb{F}_p$, dove $p = 2^{256} - 2^{32} - 977$. L'equazione della curva è:

$$y^2 \equiv x^3 + 7 \pmod{p}. \tag{1}$$

Il gruppo di punti $E(\mathbb{F}_p)$ ha ordine primo q con punto generatore G. Un'identità nella rete è rappresentata da una coppia di chiavi: la chiave privata $x \in \mathbb{F}_p$ (scalare segreto) e la corrispondente chiave pubblica $X = x \cdot G$ (punto sulla curva). Sotto l'assunzione di difficoltà del problema del logaritmo discreto su curve ellittiche (ECDLP), risalire a x a partire da X è computazionalmente infattibile.

Firme Digitali. Bitcoin implementa nativamente lo schema ECDSA (*Elliptic Curve Digital Signature Algorithm*) per autorizzare le transazioni [6]. L'aggiornamento Taproot [22–24] ha successivamente introdotto le firme Schnorr, che offrono vantaggi significativi in termini di efficienza e aggregabilità delle firme.

1.2 Il Modello della Timechain

La rete opera secondo il modello UTXO (*Unspent Transaction Output*), in cui lo stato globale è definito dall'insieme delle uscite non ancora spese.
Un output è una tupla

$$out := (a,\ lockScript),$$

composta da una quantità $a \in \mathbb{N}$ di `satoshi` (1 `satoshi` $= 10^{-8}$ BTC) e dalle condizioni di spesa *lockScript*. Un input

$$in := (PrevTx,\ outIndex,\ unlockScript)$$

identifica univocamente un output esistente, referenziando la transazione precedente e il relativo indice. Formalmente, una transazione è la tupla

$$Tx := (inputs,\ witness,\ outputs).$$

Lo script di blocco, espresso nell'apposito linguaggio di scripting, viene eseguito fornendo i dati del *witness* come parametri di input. Affinché una transazione sia considerata valida, l'esecuzione di tale script deve restituire `True` per tutti gli input, ciò valida ogni singolo input della transazione.

Possiamo definire lo stato globale Σ_t al tempo t come l'insieme degli UTXO non ancora spesi. Un singolo UTXO è una tupla $u = (v, S)$, dove v è il valore in `satoshi` e S è lo *ScriptPubKey*, ovvero la condizione di blocco. Una transazione tx non è altro che una funzione di transizione di stato δ:

$$\Sigma_{t+1} = \delta(\Sigma_t, tx) = (\Sigma_t \backslash I_{tx}) \cup O_{tx} \tag{2}$$

dove $I_{tx} \subseteq \Sigma_t$ è l'insieme degli input spesi e O_{tx} è l'insieme dei nuovi output generati, soggetti al vincolo di conservazione del valore $\sum_{u \in I_{tx}} u.v \geqslant \sum_{u \in O_{tx}} u.v$.

Sia $\mathcal{B}$ l'insieme di tutti i blocchi validi. Un blocco $B_i \in \mathcal{B}$ è una tupla (h_{i-1}, txs, n, t), dove h_{i-1} è l'hash del blocco precedente, txs è l'insieme delle transazioni, n è il nonce e t è il timestamp. Sia $H : \{0,1\}^* \to \{0,1\}^{256}$ una funzione di hash (e.g. `SHA-256`), la condizione di validità PoW per un blocco è:

$$H(B_i) \leqslant T \tag{3}$$

dove T è il target di difficoltà, aggiustato dinamicamente ogni 2016 blocchi affinché il tempo medio di generazione di un blocco sia di $\Delta t \approx 10$ minuti.

1.3 Condizioni di Spesa

Il linguaggio di scripting di Bitcoin è uno stack-based language non Turing-completo, progettato per semplicità e sicurezza. Gli script permettono diverse logiche di sblocco combinabili tra loro:

- **Firme singole (`CheckSig`):** l'output è spendibile fornendo una firma valida per la chiave pubblica associata all'indirizzo.
- **Multifirme (`CheckMultisig`):** richiedono una soglia k di n firme per validare la transazione.
- **Timelocks:** bloccano l'output fino a un momento futuro assoluto (`AbsTimelock`) o relativo al momento in cui la transazione viene inclusa on-chain (`RelTimelock`).
- **Taproot Trees:** rendono l'UTXO spendibile soddisfacendo una singola condizione tra molteplici alternative organizzate in un Merkle tree [23].

1.4 Il Trilemma della Blockchain e i Limiti di Throughput

Definition 1 (Trilemma della Blockchain). *In una rete decentralizzata è possibile ottimizzare simultaneamente soltanto due delle tre proprietà:*

- ***Decentralizzazione:*** *nessun singolo attore può controllare la maggioranza delle risorse della rete.*
- ***Sicurezza:*** *la rete è resistente ad attacchi malevoli e garantisce l'integrità del registro anche in presenza di nodi compromessi.*
- ***Scalabilità:*** *la rete può gestire un numero crescente di transazioni senza degradare le prestazioni o aumentare i costi in modo inaccettabile.*

Bitcoin privilegia decentralizzazione e sicurezza, sacrificando la scalabilità. Il throughput teorico τ (transazioni al secondo) dipende dalla dimensione massima del blocco

$\beta_{\max}$, dall'intervallo medio di generazione Δt e dalla dimensione attesa di una transazione:

$$\tau := \frac{\beta_{\max}}{\Delta t \cdot \mathbb{E}[\mathtt{tx}_{size}]}. \tag{4}$$

Un incremento arbitrario di $\beta_{\max}$ aumenta il ritardo di propagazione t_{prop}, innalzando la probabilità di blocchi orfani $P_{\text{orphan}} = 1 - e^{-\tau \cdot t_{\text{prop}}}$ [3], il che induce inevitabilmente centralizzazione nel mining. La sfida consiste quindi nel migliorare τ senza alterare i parametri fondamentali di consenso.

2 Ottimizzazioni On-Chain

Per aumentare il throughput τ senza modificare Δt né $\beta_{\max}$ direttamente, occorre ridurre $\mathtt{tx}_{size}$. Le soluzioni on-chain mirano a ottimizzare l'uso dello spazio blocco o a modificare la struttura delle transazioni per consentire logiche più complesse.

2.1 Segregated Witness (SegWit)

Attivato nel 2017 tramite *soft fork* (BIP141 [13], un aggiornamento retrocompatibile del protocollo), SegWit introduce due innovazioni strutturali fondamentali: una nuova metrica dimensionale per le transazioni (i *vBytes*) e la segregazione dei dati di firma dal corpo principale della transazione.

In una transazione **pre-SegWit**, ogni input contiene internamente lo *scriptSig*, ossia i dati di sblocco (firma e chiave pubblica) necessari a soddisfare lo *scriptPubKey* dell'output che si vuole spendere. Il TXID viene calcolato sull'intera transazione, firma inclusa. Questa struttura presenta due criticità rilevanti:

1. **Transaction malleability:** poiché ECDSA ammette firme distinte per lo stesso messaggio, se (R, s) è valida anche $(R, -s \bmod n)$ lo è, un attore poteva modificare il *scriptSig* (e quindi il TXID) senza invalidare la transazione. Ciò rendeva impossibile costruire contratti multi-step sicuri che referenziano il TXID di una transazione non ancora confermata.
2. **Quadratic hashing:** la validazione di ogni firma richiedeva di serializzare l'intera transazione, portando la complessità a $O(N^2)$ per N input, e aprendo la porta ad attacchi DoS (Denial of Service) tramite transazioni appositamente costruite.

In una transazione **post-SegWit**, i dati di firma vengono spostati in un campo separato, il *witness*, segregato dal corpo principale della transazione. La struttura logica si articola in due componenti distinti:

$$Tx = (BaseTx, WitnessTx)$$

dove:

$$BaseTx = (version,\ inputs,\ outputs,\ locktime)$$
$$WitnessTx = (marker,\ flag,\ witness_1,\ \ldots,\ witness_N)$$

Il primo componente, i *base data*, replica la struttura delle transazioni legacy ed è l'unico elemento utilizzato per il calcolo del *TXID*. Questo è il meccanismo fondamentale con cui SegWit elimina la *transaction malleability*: poiché i dati di firma risiedono nel *witness* e non nei *base data*, modificarli non altera il *TXID*, rendendo impossibile alterare l'identificatore di una transazione senza invalidarla.

Il secondo componente, i *witness data*, contiene le firme e gli script di sblocco precedentemente inclusi negli input. Per tenere traccia dell'intera transazione, inclusa la componente witness, viene introdotto il *wTXID*, calcolato sull'intera struttura. I *wTXID* vengono organizzati in un Merkle tree secondario, il cosiddetto *witness commitment*, il cui hash radice è registrato nella transazione *coinbase* del blocco.

I nodi legacy, privi di conoscenza della struttura witness, continuano a validare i blocchi come prima, ignorando i nuovi campi, essendo l'aggiornamento tramite soft fork pienamente retrocompatibile con il software preesistente.

Block Weight e vBytes. SegWit sostituisce il limite rigido di 1 MB per blocco con la metrica del *Block Weight*. A ogni byte della transazione viene assegnato un peso differente a seconda che appartenga ai *base data* o ai *witness data*:

$$W = 4 \cdot \texttt{bytes}_{base} + 1 \cdot \texttt{bytes}_{witness}. \tag{5}$$

Il blocco è valido se $W \leqslant 4\,000\,000$ WU (*Weight Units*). Questa formula può essere riscritta in modo equivalente come:

$$W = 3 \cdot \texttt{bytes}_{base} + \texttt{bytes}_{total},$$

con $\texttt{bytes}_{total} = \texttt{bytes}_{base} + \texttt{bytes}_{witness}$, dove si riconosce che i witness data contribuiscono al peso con un fattore 1 invece di 4. La dimensione virtuale, espressa in *vBytes*, normalizza il peso per preservare la compatibilità con il vecchio limite da 1 MB:

$$\text{vBytes} = \left\lceil \frac{W}{4} \right\rceil = \left\lceil \texttt{bytes}_{base} + \frac{\texttt{bytes}_{witness}}{4} \right\rceil. \tag{6}$$

Ciò equivale a uno sconto effettivo del 75% sui dati witness: un byte di firma o di script pesa quanto un quarto di un byte strutturale. Questa asimmetria è intenzionale: le fee su Bitcoin sono proporzionali ai vBytes, quindi rendere più economici i dati witness incentiva strutturalmente l'adozione di script crittograficamente complessi (multifirme, HTLC, Taproot) senza penalizzare chi li utilizza rispetto alle transazioni semplici.

Miglioramenti strutturali. SegWit risolve entrambe le criticità identificate:

- **Transaction malleability:** il TXID dipende ora solo dai base data, rendendo impossibile alterarlo senza invalidare la transazione. Questo è un prerequisito fondamentale per la sicurezza dei canali Lightning [18]: un canale LN referenzia nel suo contratto di funding il TXID di una transazione non ancora confermata, e qualsiasi alterazione di tale TXID renderebbe invalido il contratto.
- **Quadratic hashing (BIP143):** il nuovo formato di firma pre-calcola e include hash incrementali delle componenti della transazione, portando la complessità di validazione da $O(N^2)$ a $O(N)$ rispetto al numero di input N.

2.2 Taproot e Firme Schnorr

L'aggiornamento Taproot (BIP340, BIP341, BIP342 [22–24]), attivato nel novembre 2021, rappresenta il più significativo avanzamento crittografico introdotto nel protocollo Bitcoin dalla sua creazione, introducendo la possibilità di firmare transazioni usando lo schema di firma di Schnorr [20] e i Merkleized Abstract Syntax Trees (MAST).

Firme Schnorr e linearità. Lo schema di firma di Schnorr possiede la proprietà di *linearità*, che consente l'*aggregazione* di chiavi e firme. Dato un insieme di chiavi pubbliche $\{X_1, X_2, \ldots, X_n\}$, è possibile aggregarle in un'unica chiave X_{agg}, tale che una firma valida per X_{agg} autentica la transazione per tutte le singole chiavi coinvolte.

Per prevenire i *Rogue Key Attack*, dove un attore malevolo costruisce una chiave pubblica che cancella algebricamente quella degli altri partecipanti, il protocollo MuSig2 [15] utilizza coefficienti di aggregazione pesati:

$$X_{\text{agg}} = \sum_{i=1}^{n} c_i X_i, \quad c_i = H_{\text{agg}}(L \,\|\, X_i), \tag{7}$$

dove L è l'insieme lessicografico di tutte le chiavi pubbliche partecipanti e si denota con $\|$ l'operatore di concatenazione di stringhe di bit. Il risultato è che le transazioni multi-firma appaiono on-chain identiche alle transazioni a firma singola: si ottiene così un incremento simultaneo di privacy e compressione dei dati, riducendo significativamente il costo on-chain delle transazioni multi-firma.

MAST e Taproot trees. Taproot introduce i *Merkleized Abstract Syntax Trees* (MAST), che consentono di impegnarsi su script complessi senza rivelarne la logica on-chain. La chiave pubblica interna X viene modificata con la radice di un Merkle tree contenente gli script alternativi (*tapleaves*):

$$Q = X + H_{\text{TapTweak}}(X \,\|\, \mathit{MerkleRoot}) \cdot G. \tag{8}$$

Per spendere i fondi tramite uno script, è sufficiente rivelare il ramo corrispondente e la prova di appartenenza al Merkle tree, di dimensione $O(\log n)$, dove n è il numero di script alternativi. Gli script non utilizzati rimangono privati, migliorando la confidenzialità e riducendo il footprint on-chain degli smart contract complessi.

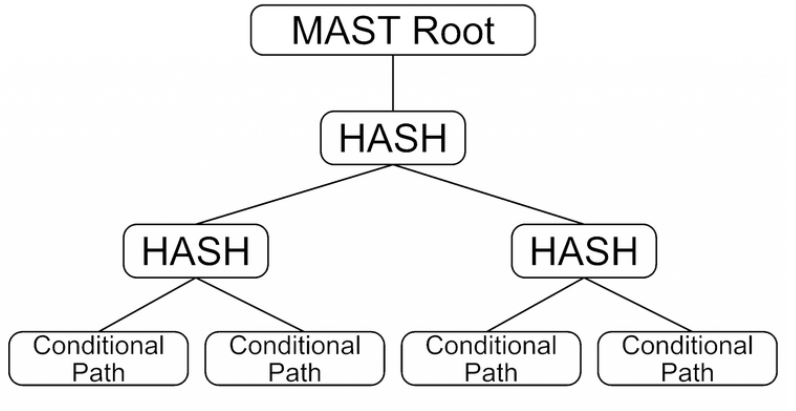


Fig. 1: Merkleized Abstract Syntax Tree (MAST).

2.3 Cross-Input Signature Aggregation (CISA)

CISA è una proposta di aggiornamento [5] che estende i benefici della linearità di Schnorr a livello di transazione, anziché di singolo input. Attualmente, ogni input richiede una firma $\sigma_i = (R_i, s_i)$ di 64 byte, per un totale di $64 \cdot N$ byte di witness data per N input. CISA mirerebbe ad aggregare le singole firme degli input $(\sigma_i)_{i=1}^{N}$ in un'unica firma globale σ_{agg} valida per tutti gli input.
Esistono due varianti:

Half-Aggregation. Solo la componente scalare s_i di ogni firma viene aggregata sfruttando un protocollo *non interattivo* [17]:

$$\sigma_{\text{agg}} = \Big((R_1, \ldots, R_N),\ s_{\text{agg}} := \textstyle\sum_{i=1}^{N} s_i \Big). \tag{9}$$

La dimensione risultante è $32N + 32$ byte: ancora lineare in N, ma con un risparmio di circa il 50% rispetto al caso non aggregato.

Full-Aggregation. Per massimizzare il risparmio di spazio, il paradigma della *Full-Aggregation* prevede l'aggregazione totale delle firme. Ciò significa che le N firme

vengono combinate in un'unica firma σ_{agg} di dimensione costante di 64 bytes (una classica firma di Schnorr) che autentica tutti gli input simultaneamente. In particolare, si sfrutta un protocollo *interattivo* [16] generando una firma finale $\sigma_{agg} = (R_{agg}, s_{agg})$. Questo approccio riduce drasticamente la dimensione della firma a 64 bytes, indipendentemente dal numero di input.

2.4 Covenants

I covenants permettono di vincolare *come* e *dove* i fondi possano essere spesi in futuro, introducendo una forma di programmabilità condizionale sul ciclo di vita degli UTXO. Proposte come `OP_CTV` (CheckTemplateVerify, BIP119 [19]) e `SIGHASH_ANYPREVOUT` (APO, BIP118 [2]) consentono di pre-calcolare l'hash delle transazioni di spesa, abilitando:

- **Congestion Control:** un singolo UTXO può essere espanso in un albero di pagamenti off-chain ed eseguito on-chain solo quando necessario, riducendo il numero di transazioni che saturano la mempool.
- **Vaults:** meccanismi di sicurezza che impongono ritardi temporali e percorsi di recupero per i fondi, proteggendo contro furti di chiavi.

I covenants sono rilevanti anche come base crittografica per i protocolli di Layer 2 che richiedono garanzie di *unilateral exit* o per implementare logiche di pagamento off-chain più sofisticate.

3 Soluzioni Off-Chain e Layer 2

Poiché la timechain deve garantire la massima sicurezza e decentralizzazione, la reale scalabilità transazionale è delegata a protocolli di Layer 2. Questi sfruttano il Layer 1 come *settlement layer* di ultima istanza, ancorandone la sicurezza termodinamica della PoW solo quando strettamente necessario, ovvero per l'apertura e la chiusura dei canali, o per la risoluzione delle dispute.

3.1 Lightning Network

La Lightning Network (LN) [18] è il primo protocollo che ha permesso di scalare Bitcoin in modo pratico. Si fonda su canali di pagamento bidirezionali tra coppie di nodi, formando un grafo diretto pesato $G(V, E)$ in cui V è l'insieme dei nodi LN ed E è l'insieme dei canali, pesati dalla liquidità allocata dalle due parti durante la creazione.

Ogni canale è aperto con una transazione on-chain che finanzia un output multi-firma 2-of-2. I successivi aggiornamenti di stato del canale avvengono esclusivamente off-chain, scambiando transazioni pre-firmate che ridistribuiscono la liquidità. La

sicurezza è garantita da transazioni di penalità: se un nodo trasmette uno stato obsoleto del canale (tentativo di frode), la controparte può confiscare l'intero saldo grazie a chiavi di revoca pre-scambiate.

LN permette pagamenti istantanei e con fee prossime allo zero, ma introduce requisiti di liquidità e l'obbligo di essere online per ricevere pagamenti (watchtowers mitigano i rischi offline).

Hashed Time-Locked Contracts (HTLC). LN utilizza gli HTLC per instradare pagamenti attraverso percorsi multi-hop senza registrare ogni transazione on-chain [18]. Un HTLC vincola i fondi a due condizioni mutuamente esclusive:

1. il destinatario rivela una preimmagine P tale che $H(P) = Hash$ entro un timeout $CLTV_Expiry$ (percorso felice);
2. scaduto il timeout, il mittente recupera i fondi (percorso di rimborso).

La sicurezza deriva dal fatto che la preimmagine P (dove $H(P) = Hash$) è inizialmente sconosciuta.

```
OP_IF
    OP_SHA256 <Hash(Preimage)> OP_EQUALVERIFY
    <Bob_Pubkey> OP_CHECKSIG
OP_ELSE
    <Cltv_Expiry> OP_CHECKLOCKTIMEVERIFY OP_DROP
    <Alice_Pubkey> OP_CHECKSIG
OP_ENDIF
```

Grazie alle firme Schnorr, LN sta evolvendo verso i **Point Time-Locked Contracts** (PTLC), che sostituiscono la preimmagine di hash con uno scalare segreto t e il suo punto sulla curva ellittica associato $T = t \cdot G$. I PTLC eliminano la correlazione crittografica tra gli HTLC di hop diversi, prevenendo attacchi di correlazione come il *wormhole attack*.

Il Protocollo di Routing. Trovare un percorso ottimale nel grafo tra mittente e destinatario richiede algoritmi di routing efficienti. Poiché i saldi dei canali sono privati e mutano continuamente, LN adotta un approccio ibrido di *Source Routing* con *Onion Routing*. Il mittente calcola il percorso completo $A \to B \to \cdots \to Z$ e cifra il pacchetto in strati: ogni nodo N_i decifra solo il proprio strato per scoprire N_{i+1}, senza conoscere l'intero percorso né l'identità del mittente o del destinatario.

Con i PTLC, il routing sfrutta le *adaptor signatures*: ogni salto nel grafo utilizza un punto $T' = T + r \cdot G$ randomizzato dal nodo intermedio, rendendo le transazioni di routing crittograficamente scollegate tra loro e migliorando sensibilmente la privacy.

3.2 Ark

Lightning Network, pur rivoluzionaria, presenta frizioni strutturali che ne limitano l'adozione di massa. Il problema della *liquidità in entrata* impone al ricevente di avere fondi già allocati verso di sé in canali aperti da terzi; il requisito di *liveness* obbliga ogni nodo ad essere online per ricevere pagamenti, delegando la sorveglianza a watchtower esterne in caso contrario. Ark [7] affronta entrambi questi problemi con un modello architetturale radicalmente diverso.

ASP e UTXO Virtuali. Ark introduce la figura dell'*Ark Service Provider* (ASP), un operatore di liquidità sempre online che funge da coordinatore centralizzato ma *non custodiale*. Gli utenti non detengono UTXO on-chain diretti, bensì *UTXO virtuali* (vTXO): foglie di un albero binario off-chain la cui radice è ancorata a una singola transazione on-chain periodica, detta *pool transaction*.
La pool transaction viene emessa dall'ASP ogni *round* e finanzia due output:

- un output che impegna la radice dell'albero dei vTXO del round corrente;
- un output di connettore che lega atomicamente il round corrente al precedente, garantendo la continuità della catena di custodia.

Ogni vTXO è una foglia dell'albero identificata da una coppia (v, pk), dove v è il valore in `satoshi` e pk è la chiave pubblica del proprietario. L'ASP conosce la struttura dell'albero e può rivelare qualsiasi ramo, ma non può spendere i vTXO altrui poiché ogni foglia è protetta dalla chiave del proprietario.

Unilateral Exit. La proprietà fondamentale che distingue Ark dalle sidechain federate è la **Unilateral Exit**: ogni utente può forzare unilateralmente la pubblicazione on-chain del proprio ramo dell'albero, anche in assenza di cooperazione dell'ASP.

Il meccanismo si basa su un covenant che vincola l'ASP a rivelare l'intero percorso dalla radice alla foglia dell'utente entro un timeout. Con `OP_CTV` [19], questo covenant è nativo: la pool transaction pre-impegna l'hash dell'albero figlio, e ogni nodo interno pre-impegna i propri figli, rendendo la struttura completamente verificabile on-chain senza cooperazione dell'ASP. In assenza di covenants nativi, Ark emula questo comportamento con script pre-firmati tra ASP e utenti, introducendo un'assunzione di liveness minima sull'ASP solo durante il round di apertura.

Se l'ASP smette di cooperare o sparisce, l'utente ha un percorso di exit garantito: pubblica on-chain il proprio ramo, attendendo la scadenza del timelock relativo. Il costo di questa operazione è $O(\log n)$ transazioni, dove n è il numero di vTXO nel round, significativamente inferiore all'apertura di un canale LN dedicato.

Pagamenti in Ark. Un pagamento in Ark attraversa tre fasi distinte:

1. **Boarding:** un nuovo utente invia una transazione on-chain all'ASP, che include il suo UTXO nel prossimo round. Il boarding è atomico: l'utente ottiene un

vTXO nel nuovo albero solo se la sua transazione on-chain viene inclusa nella pool transaction del round. Non esiste una fase di negoziazione del canale come in LN.

2. **Pagamento off-chain:** per pagare un altro utente nello stesso round, il mittente firma la cessione del proprio vTXO al destinatario. L'ASP coordina la transazione includendo il nuovo vTXO del destinatario nel round successivo e invalidando atomicamente il vTXO del mittente tramite il meccanismo dei connettori. A differenza di LN, il destinatario non deve essere online al momento del pagamento: riceve semplicemente un vTXO nel round successivo.
3. **Exit:** per tornare on-chain, l'utente può attendere la scadenza del proprio vTXO (exit cooperativa con l'ASP, costo minimo) oppure attivare la Unilateral Exit pubblicando il proprio ramo dell'albero in caso di inadempienza dell'ASP.

Interoperabilità ed impatto. Ark e LN non sono protocolli in competizione, ma complementari: LN è ottimale per pagamenti frequenti e bidirezionali tra nodi con liquidità pre-allocata; Ark è ottimale per riceventi passivi, pagamenti asincroni e utenti che non possono mantenere un nodo sempre online.

Dal punto di vista della scalabilità, il contributo di Ark è strutturalmente diverso da quello di LN. Mentre LN elimina le transazioni on-chain per i pagamenti tra nodi connessi, Ark le aggrega: n pagamenti off-chain producono una singola pool transaction on-chain per round, con un footprint pari a $O(1)$ transazioni indipendentemente dal numero di partecipanti al round. Con round frequenti e molti partecipanti, il throughput effettivo è limitato solo dalla capacità dell'ASP di coordinare i round, non dai parametri di consenso del Layer 1.

3.3 BitVM: Verificabilità Computazionale su Bitcoin

BitVM [10] rappresenta un cambio di paradigma verso la verificabilità di calcoli arbitrari (Turing-completi) su Bitcoin, senza modificare il protocollo tramite soft fork. Il paradigma adottato è quello degli *Optimistic Rollup*: il calcolo avviene off-chain, il risultato è asserito on-chain, e la blockchain interviene *solo* in caso di disputa tra il *Prover* $\mathcal{P}$ e il *Verifier* $\mathcal{V}$.

Utilizzando Taproot, il circuito logico del programma è suddiviso in miliardi di foglie (Tapleaves). In caso di disputa, la blockchain esegue solo le poche istruzioni logiche (porte NAND) necessarie per verificare la frode. Questo apre le porte a bridge trustless e sidechain più sicure.

Bit Value Commitment. La base crittografica di BitVM è il *bit commitment*. Il Prover $\mathcal{P}$ genera due segreti s_0, s_1 e impegna un bit $b \in \{0, 1\}$ pubblicando i rispettivi hash

$$H_0 = H(s_0) \quad \text{e} \quad H_1 = H(s_1).$$

Per rivelare b, $\mathcal{P}$ divulga esclusivamente la preimmagine di H_b, cioè s_b e non s_{1-b}. Se $\mathcal{P}$ dovesse rivelare entrambe le preimmagini (*equivocation*), il Verifier $\mathcal{V}$ può attivare un ramo del TapTree che gli consente di confiscare il deposito di garanzia.

Logic Gate Commitment. L'intera logica del programma da eseguire è mappata su porte NAND, che costituiscono una base funzionalmente completa per la logica booleana. Ciascuna porta NAND con input A, B e output C è impegnata dal Prover come foglia Taproot (*tapleaf*), che modella la relazione:

$$C = \neg(A \wedge B). \tag{10}$$

La struttura Taproot permette di committarsi a miliardi di porte logiche senza che queste vengano mai pubblicate on-chain nell'uso ordinario.

Gestione delle Dispute. Poiché un intero programma è troppo grande per essere verificato in un singolo blocco, BitVM sfrutta un protocollo di sfida interattivo (*bisection game*). Se il programma richiede k passi di esecuzione:

1. Il Verifier $\mathcal{V}$ contesta il risultato finale richiedendo a $\mathcal{P}$ di rivelare lo stato intermedio al passo $k/2$.
2. $\mathcal{V}$ determina se l'errore risiede nella metà superiore o inferiore.
3. Il processo si ripete ricorsivamente, dimezzando lo spazio di ricerca ad ogni round.

La complessità on-chain è $O(\log_2 k)$: al termine viene pubblicata esclusivamente la singola porta NAND eseguita scorrettamente, e il Layer 1 sanziona la frode in una singola transazione. Il protocollo originale è tuttavia *two-party*: richiede un Verifier dedicato per ogni Prover, con $O(\log_2 k)$ round di interazione preventivamente coordinati.

BitVM2: Firme di Lamport, Checkpoint e Verifica Permissionless. La prima limitazione del design originale è affrontata da BitVM2 [12], che riduce l'interazione a soli *due round* (challenge e response) grazie alle *Firme di Lamport* [8].

Le Firme di Lamport sono schemi di firma one-time basati esclusivamente su funzioni hash. Per firmare un messaggio m di ℓ bit, il firmatario:

1. genera 2ℓ segreti casuali $x[b, i]$ con $b \in \{0, 1\}$, $i \in \{1, \ldots, \ell\}$, e pubblica i rispettivi hash $y[b, i] = H(x[b, i])$ come chiave pubblica;
2. firma rivelando, per ciascun bit $m[i]$, esattamente una delle due preimmagini $x[m[i], i]$.

Un tentativo di equivocazione, cioè rivelare entrambe le preimmagini per lo stesso bit, è immediatamente rilevabile e sanzionabile on-chain.

Hardcodando le chiavi pubbliche di Lamport negli script degli output Taproot, BitVM2 vincola il Prover a impegnarsi su un numero costante di *checkpoint* di

stato intermedi, collegati crittograficamente tra loro tra tapleaf diverse. In fase di sfida, $\mathcal{V}$ identifica immediatamente il checkpoint inconsistente e richiede a $\mathcal{P}$ di eseguire on-chain solo il blocco corrispondente, eliminando la necessità di bisecare ricorsivamente.

Questo rende la verifica *permissionless*: chiunque, senza coordinamento preventivo con $\mathcal{P}$, può rilevare una frode, sottomettere la challenge e riscuotere la penalità. L'assunzione di sicurezza scende a 1-of-N: è sufficiente che un solo osservatore onesto tra N sia attivo. La prima applicazione concreta è il **BitVM Bridge** [12], un bridge trustless con altre sidechain basato sul *peg-out ottimistico*: un operatore anticipa i fondi in uscita e reclama il rimborso presentando una prova di correttezza che chiunque può contestare on-chain, senza richiedere fiducia in un insieme federato di custodi.

BitVMX e BitVM3. Le evoluzioni successive ampliano ulteriormente l'espressività del sistema e ne semplificano il setup.

BitVMX [9] sostituisce la rete di porte NAND con una CPU *RISC-V* come circuito verificabile, permettendo di compilare programmi in C o Rust con toolchain standard, senza dover ridurre manualmente la logica a porte elementari. Questo abbassa drasticamente la barriera tecnica allo sviluppo di applicazioni, avvicinando Bitcoin a un modello di programmabilità più ricco senza alterare le garanzie sottostanti.

BitVM3s ([21], [11]) affronta il problema del setup interattivo ricorrendo ai *garbled circuits* di Yao [25]: il Prover costruisce off-chain un circuito "ingarbugliato" che il Verifier può valutare senza conoscere gli input del Prover, eliminando la necessità di scambiare informazioni fuori banda. Questo rende il setup completamente non interattivo e riduce sensibilmente il numero di tapleaf necessarie al commitment.

SNARG e ZK-Rollup. BitVM può integrare *Succinct Non-interactive Arguments* (SNARG) [1]. Un sistema SNARG è specificato da tre algoritmi:

- $\mathit{SNARG.Setup}(R)$: genera la stringa di riferimento comune (CRS) per la relazione R;
- $\mathit{SNARG.Prove}(R, \mathit{crs}, \phi, w)$: produce un argomento crittografico π a partire dall'asserzione ϕ e dal testimone w;
- $\mathit{SNARG.Vrfy}(R, \mathit{crs}, \phi, \pi)$: verifica la validità di π.

Il programma da verificare diventa il verificatore $\mathit{SNARG.Vrfy}$ stesso, permettendo a Bitcoin di validare prove Zero-Knowledge in tempo $O(\log_2 k)$ on-chain e aprendo la strada a ZK-Rollup nativi ancorati alla PoW.

Dal punto di vista della scalabilità, il contributo di questa linea di ricerca è chiaro: BitVM e le sue evoluzioni rendono praticabile la costruzione di bridge e sidechain con garanzie ancorate alla PoW di Bitcoin, su cui spostare volumi transazionali altrimenti impossibili da gestire sul Layer 1.

4 Conclusioni

La tensione al centro del dibattito sulla scalabilità non è solamente tecnica ma filosofica: come aumentare la portata di un sistema la cui forza deriva precisamente dalla sua resistenza al cambiamento. Bitcoin non può essere reso scalabile modificandone i parametri fondamentali senza alterare le proprietà che lo rendono *hard money*, come immutabilità, prevedibilità dell'emissione, resistenza alla censura. La risposta che emerge dalla ricerca è che questa tensione è risolvibile attraverso l'interoperabilità tra livelli, a condizione che ogni livello superiore erediti le garanzie del sottostante senza richiederne modifiche: sul Layer 1, SegWit e Taproot non allargano il blocco ma massimizzano la densità informativa di ogni byte; sul Layer 2, LN e Ark spostano la frequenza transazionale off-chain preservando la riducibilità alla PoW; infine, BitVM estende questa proprietà alle sidechain, trasformando Bitcoin da registro a giudice di verità computazionale.

Questa condizione di eredità crittografica non è scontata. I bridge federati, storicamente, l'hanno violata: spostare bitcoin verso una sidechain significava affidarsi a un multisig k-of-N di custodi, introducendo un punto di fallimento esterno alla PoW. BitVM e le sue evoluzioni rompono questo compromesso: una sidechain ancorata tramite BitVM Bridge non usa Bitcoin come semplice asset, ma ne eredita la sicurezza con assunzioni di fiducia ridotte a 1-of-N.

L'interoperabilità tra i protocolli Layer 2 stessi è altrettanto cruciale e ancora largamente aperta. LN e Ark risolvono problemi complementari, il primo ottimale per pagamenti frequenti e bidirezionali tra nodi connessi, il secondo per riceventi passivi e pagamenti asincroni, ma operano oggi in modo sostanzialmente indipendente. La capacità di scambiare atomicamente vTXO Ark con liquidità LN esiste in linea di principio, ma richiede un coordinamento crittografico tra i due sistemi che la ricerca non ha ancora standardizzato. Analogamente, l'integrazione tra ZK-Rollup ancorati tramite BitVM e canali LN aprirebbe la strada a pagamenti istantanei con finalità garantita dalla PoW: una combinazione oggi non disponibile su nessun sistema monetario digitale.

Il proseguimento della ricerca e del dibattito sui covenants è in questo senso determinante. Primitive come `OP_CTV` o `OP_CAT` [4] non sono semplici ottimizzazioni dello spazio blocco: sono il linguaggio con cui il Layer 1 può esprimere vincoli sullo stato futuro degli UTXO, rendendo trustless ciò che oggi richiede pre-firma. Senza di essi Ark dipende dall'ASP come co-firmatario, BitVM richiede un setup interattivo, e la composizione tra protocolli Layer 2 diversi rimane fragile. Con essi, la fiducia richiesta a ogni livello converge verso zero pur mantenendo intatta la base termodinamica del Layer 1.

La posta in gioco è alta: Bitcoin come infrastruttura monetaria globale non è raggiungibile con le poche transazioni al secondo del Layer 1, ma è ugualmente irraggiungibile con soluzioni che ne diluiscono le proprietà fondamentali per guadagnare throughput. La direzione imboccata dalla ricerca è l'unica che preserva entrambe le esigenze, e la velocità con cui convergerà in protocolli maturi dipende dalla volontà della comunità di continuare a sviluppare primitive e aggiornamenti consensuali che amplino l'espressività del Layer 1 senza comprometterne l'invariante più profondo: nessuno può spendere ciò che non gli appartiene.

References

1. Eli Ben-Sasson, Alessandro Chiesa, Daniel Genkin, Eran Tromer, and Madars Virza. Snarks for c: Verifying program executions succinctly and in zero knowledge. In *Annual cryptology conference*, pages 90–108. Springer, 2013.
2. Christian Decker and Anthony Towns. BIP118: SIGHASH_ANYPREVOUT for Taproot Scripts. `https://github.com/bitcoin/bips/blob/master/bip-0118.mediawiki`, 2017.
3. Christian Decker and Roger Wattenhofer. Information Propagation in the Bitcoin Network. In *13th IEEE International Conference on Peer-to-Peer Computing (P2P)*, pages 1–10, 2013.
4. Ethan Heilman, Victor Kolobov, Andrew Poelstra, and Pieter Wuille. BIP347: OP_CAT. `https://github.com/bitcoin/bips/blob/master/bip-0347.mediawiki`, 2023.
5. Fabian Jahr. Cross-input signature aggregation for bitcoin. Cisa research paper, Human Rights Foundation, March 2025. HRF CISA Fellowship.
6. Don Johnson, Alfred Menezes, and Scott Vanstone. The Elliptic Curve Digital Signature Algorithm (ECDSA). *International Journal of Information Security*, 1(1):36–63, 2001.
7. Pim Keer, Matteo Maffei, Marco Argentieri, Andrew Camilleri, and Zeta Avarikioti. Ark: Offchain transaction batching in bitcoin. *arXiv preprint arXiv:2605.20952*, 2026.
8. Leslie Lamport. Constructing Digital Signatures from a One-Way Function. Technical Report CSL-98, SRI International, 1979.
9. Sergio Demian Lerner, Ramon Amela, Shreemoy Mishra, Martin Jonas, and Javier Álvarez Cid-Fuentes. Bitvmx: A cpu for universal computation on bitcoin. *arXiv preprint arXiv:2405.06842*, 2024.
10. Robin Linus. BitVM: Compute Anything on Bitcoin. `https://bitvm.org/bitvm.pdf`, 2023.
11. Robin Linus. Bitvm 3s–garbled circuits for efficient computation on bitcoin, 2025.
12. Robin Linus, Lukas Aumayr, Alexei Zamyatin, Andrea Pelosi, Zeta Avarikioti, and Matteo Maffei. Bitvm2: Bridging bitcoin to second layers. *URL: https://bitvm.org/bitvm_bridge. pdf*, 2024.
13. Eric Lombrozo, Johnson Lau, and Pieter Wuille. BIP 141: Segregated witness (consensus layer). Technical report, Bitcoin Improvement Proposal, 2015.
14. Satoshi Nakamoto. Bitcoin whitepaper. *URL: https://bitcoin.org/bitcoin.pdf*, 9:15, 2008.

15. Jonas Nick, Tim Ruffing, and Yannick Seurin. MuSig2: Simple Two-Round Schnorr Multi-Signatures. In *Advances in Cryptology – CRYPTO 2021*, volume 12825 of *Lecture Notes in Computer Science*, pages 189–221. Springer, 2021.
16. Jonas Nick, Tim Ruffing, and Yannick Seurin. Dahlias: Discrete logarithm-based interactive aggregate signatures. *Cryptology ePrint Archive*, 2025.
17. Jonas Nick, Tim Ruffing, Yannick Seurin, and Elliott Jin. Half-Aggregation of BIP-340 Schnorr Signatures. `https://github.com/BlockstreamResearch/cross-input-aggregation`, 2023.
18. Joseph Poon and Thaddeus Dryja. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. `https://lightning.network/lightning-network-paper.pdf`, 2016.
19. Jeremy Rubin. BIP119: CHECKTEMPLATEVERIFY. `https://github.com/bitcoin/bips/blob/master/bip-0119.mediawiki`, 2020.
20. Claus-Peter Schnorr. Efficient Signature Generation by Smart Cards. *Journal of Cryptology*, 4(3):161–174, 1991.
21. Robin Linus Woll, Ioannis Alexopoulos, Lukas Aumayr, Zeta Avarikioti, Matteo Maffei, and David Tse. Bitvm3: Efficient bitcoin bridges via garbled circuits. *Cryptology ePrint Archive*, 2026.
22. Pieter Wuille, Jonas Nick, and Tim Ruffing. BIP340: Schnorr Signatures for secp256k1. `https://github.com/bitcoin/bips/blob/master/bip-0340.mediawiki`, 2020.
23. Pieter Wuille, Jonas Nick, and Anthony Towns. BIP 341: Taproot: Segwit v1 sigpubkey scripts. Technical report, Bitcoin Improvement Proposal, 2020.
24. Pieter Wuille, Jonas Nick, and Anthony Towns. BIP342: Validation of Taproot Scripts. `https://github.com/bitcoin/bips/blob/master/bip-0342.mediawiki`, 2020.
25. Andrew Chi-Chih Yao. How to generate and exchange secrets. In *27th annual symposium on foundations of computer science (Sfcs 1986)*, pages 162–167. IEEE, 1986.

Wallet e indirizzi in Bitcoin

Enrico Zangirolami

BitPolito, Politecnico di Torino, Italy

Abstract. L'architettura decentralizzata di Bitcoin offre agli utenti la possibilità di avere la responsabilità esclusiva della custodia dei propri fondi, spostando il paradigma di sicurezza dall'affidamento a terze parti alla gestione diretta di segreti crittografici. Questo articolo fornisce un'analisi tecnica del funzionamento dei wallet Bitcoin, disaggregando le componenti principali che permettono la generazione, l'archiviazione e l'utilizzo delle chiavi all'interno del wallet.

L'articolo si concentra sullo studio del funzionamento dei wallet moderni, definiti secondo lo standard BIP32. Si dettaglia come questa struttura deterministica permetta la generazione di un numero virtualmente infinito di coppie di chiavi a partire da un'unica chiave master iniziale, collocandole gerarchicamente in un albero logico che semplifica drasticamente le procedure di backup.

Più in generale, emerge come nel tempo la ricerca in questo campo sia stata orientata verso la semplificazione dell'esperienza dell'utente, a partire dallo standard BIP39, che funge da ponte tra la complessità matematica delle chiavi crittografiche e la necessità di accedere facilmente ai propri fondi. Viene analizzato l'algoritmo che converte l'entropia iniziale in una sequenza mnemonica leggibile di 12 o 24 parole (la seed phrase) che l'utente deve ricordare per poter derivare autonomamente tutto il contenuto del wallet. Allo stesso modo viene esplorata la sintassi e la logica dei Derivation Path. Viene spiegato come questi percorsi deterministici guidino l'organizzazione semantica dei fondi e come vengono integrati all'interno della maggior parte dei wallet oggi esistenti.

Keywords: wallet · seed phrase · chiavi estese · Child Key Derivation function · PRNG

De Cifris Koine – BITCOIN & BLOCKCHAIN
https://doi.org/10.69091/koine/vol-6-B04

1 HD Wallet

Un wallet gerarchico deterministico (o più semplicemente HD Wallet, da *Hierarchical Deterministic Wallet*) è essenzialmente un wallet in grado di generare tutte le sue chiavi e indirizzi a partire da un'unica sorgente. Questa tecnologia, introdotta nel 2012 con BIP 32 [14], è adottata nella quasi totalità dei wallet moderni, a partire da Electrum e Sparrow fino a dispositivi hardware come Trezor o Coldcard.

La nomenclatura descrive due caratteristiche fondamentali:

- **Gerarchico**: Le chiavi e gli indirizzi possono essere organizzati secondo una struttura gerarchica.
- **Deterministico**: Le chiavi e gli indirizzi sono generati sempre nello stesso modo.

In sostanza, un HD Wallet permette all'utente di generare miliardi di chiavi private a partire da una singola sorgente di entropia: il *seed*. Finché si conserva il seed, è possibile ricavare la **chiave master** e tutte le chiavi figlie in modo deterministico.

Grazie a questa proprietà, questo sistema risulta molto più efficiente e facile da utilizzare rispetto a un semplice wallet non-deterministico, nel quale l'utente deve invece generare indipendentemente una nuova chiave ogni volta che ne ha bisogno.

Le caratteristiche che rendono gli HD Wallet una tecnologia tanto vantaggiosa sono dunque le seguenti:

1. **Backup Singolo**: Come detto, in un wallet di base, ogni volta che si desidera ricevere un pagamento, viene generata indipendentemente una nuova coppia di chiave privata e pubblica. Benché funzionale, questo metodo richiede di effettuare un backup del wallet ogni volta che si riceve un nuovo pagamento. Per un HD Wallet, l'unico backup necessario è quello del seed.
2. **Organizzazione**: La natura gerarchica permette a ogni chiave figlia di generare a sua volta nuove chiavi. Questo consente di creare una struttura ad albero per organizzare le chiavi in diversi rami logici.
3. **Generazione indipendente di chiavi pubbliche**: Una caratteristica peculiare è che la chiave pubblica master può generare le stesse chiavi pubbliche figlie della chiave privata master, ma senza rivelare le rispettive chiavi private. Questo permette, ad esempio, di installare la chiave pubblica master su un server web (come un e-commerce) per generare nuovi indirizzi di ricezione, mantenendo le chiavi private al sicuro in un dispositivo offline (*cold storage*).

1.1 Chiavi estese

Il processo di generazione delle chiavi segue passaggi matematici precisi.

Inizialmente, vengono generati 64 byte casuali, che costituiscono il seed vero e proprio. Dal momento che ogni chiave sarà derivata in maniera deterministica a partire da questo valore, possiamo dire che il seed identifica univocamente un

wallet, per cui un wallet qualsiasi è concettualmente equivalente a una determinata sequenza di 512 bit.

A questo punto viene utilizzata la funzione HMAC-SHA512 [1] per ricavare la chiave master, che è quella da cui si potranno ottenere tutte le chiavi dei livelli gerarchici successivi:

1. Si inserisce il seed come dato e la stringa arbitraria "Bitcoin seed" come chiave nella funzione HMAC.
2. La funzione restituisce 64 byte di output imprevedibile, che vengono suddivisi in due metà:
   - I primi 32 byte diventano la chiave privata master.
   - Gli ultimi 32 byte diventano il ***chain code***.

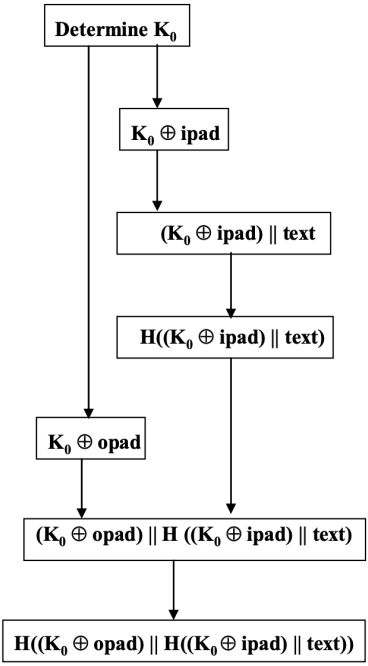


Fig. 1: Schema del funzionamento di HMAC. Immagine tratta da [12].

[1] HMAC (*Hash-based Message Authentication Code*) [3] è un costrutto specifico che utilizza una funzione di hash, che in questo caso è SHA-512 [6], in combinazione con una chiave segreta per proteggere sia l'integrità dei dati che l'autenticità del mittente.

Osserviamo che, in realtà, questo passaggio iniziale è apparentemente superfluo, poiché avremmo potuto usare direttamente i 64 byte del seed senza passare per HMAC-SHA512; questa operazione è effettuata più che altro per motivi di coerenza con il processo di derivazione delle chiavi nei livelli successivi.

In generale, la coppia formata da una normale chiave privata K e il relativo chain code c forma quella che viene definita **chiave estesa** (K, c). Una chiave estesa è in grado di produrre nuove chiavi all'interno del wallet. Il chain code è invece essenziale per la sicurezza, poiché impedisce a un attaccante di calcolare le chiavi discendenti, anche se conosce la chiave privata del padre.

Tutte le chiavi estese possono generare chiavi estese figlie, ciascuna identificata da un indice che varia da 0 fino a 4.294.967.295 (cioè $2^{32} - 1$).

Esistono due tipologie di derivazione basate sull'intervallo del valore dell'indice:

- **Derivazione Normale** (Indici compresi tra 0 e $2^{31} - 1$): Permette alla chiave pubblica estesa di derivare le chiavi pubbliche figlie.
- **Derivazione *Hardened*** (Indici compresi tra 2^{31} e $2^{32} - 1$): Solo la chiave privata estesa può generare le chiavi figlie. Le chiavi pubbliche estese non possono derivare nulla in questo intervallo.

Teoricamente, quindi, ogni chiave estesa all'interno dell'albero può avere fino a 4.294.967.296 chiavi figlie distinte, di cui esattamente metà sono hardened (per un utente è come se fossero praticamente infinite).

1.2 Meccanismi di Derivazione dei Figli

Il processo di derivazione delle chiavi figlie a partire da una chiave estesa è uno degli aspetti più rilevanti e matematicamente interessanti dell'architettura degli HD wallet.

Le *Child Key Derivation* (CKD) *functions* implementano gli algoritmi utilizzati per il calcolo delle chiavi figlie e variano a seconda che la derivazione sia hardened o meno.

Derivazione normale da chiave privata estesa Per creare un figlio da una chiave privata estesa genitore (k_{par}, c_{par}), la funzione $CKDpriv$ opera nel seguente modo:

1. Si calcola la chiave pubblica del genitore K_{par}.
2. Si inseriscono come input di HMAC K_{par}, l'indice i del figlio $(0 \leqslant i \leqslant 2^{31} - 1)$ e il chain code c_{par}.
3. I primi 32 byte dell'output vengono sommati (aritmetica scalare) k_{par} per ottenere la chiave privata figlia k_i.
4. Gli ultimi 32 byte diventano il nuovo chain code c_i del figlio.

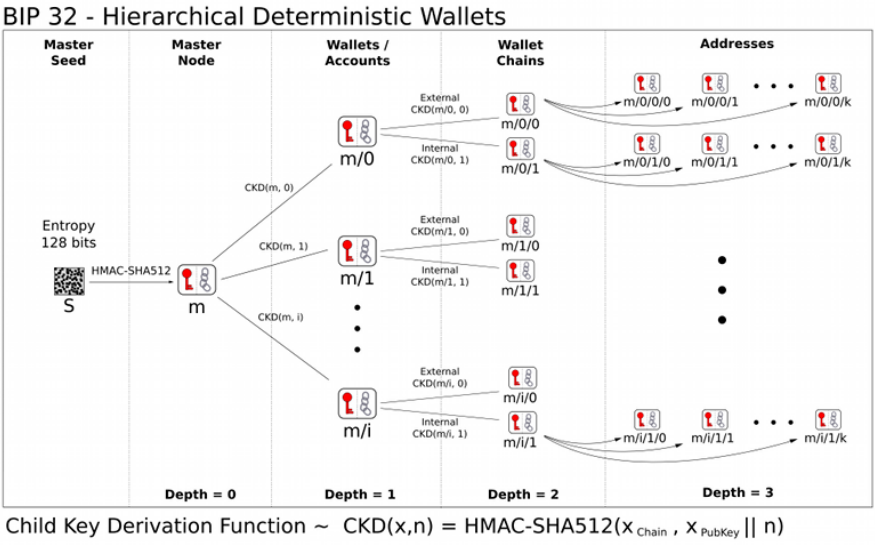


Fig. 2: Schema dell'albero di derivazione delle chiavi in un HD wallet. Immagine tratta da [14].

Derivazione hardened da chiave privata estesa La derivazione hardened (letteralmente "indurita") differisce da quella normale nel dato di input:

1. Si inserisce come input di HMAC direttamente la chiave privata k_{par} del genitore (invece della pubblica) insieme all'indice i (appartenente all'intervallo $2^{31} \leqslant i \leqslant 2^{32} - 1$) e al chain code c_{par}.
2. Il risultato viene sommato alla chiave privata del genitore. Questo consente di ottenere la chiave figlia.

Dal momento che, in questo caso, è richiesta la chiave privata del genitore come input, una chiave pubblica estesa non potrà mai derivare figli hardened.

Derivazione da chiave pubblica estesa Questa caratteristica è fondamentale nel contesto degli HD wallet. Poiché la derivazione normale utilizza la chiave pubblica del genitore come input di HMAC, una chiave pubblica estesa contiene tutti i dati necessari per replicare il processo. Attraverso l'aritmetica dei punti sulla curva ellittica [7], è possibile sommare il risultato di HMAC (convertito in un punto sulla curva) con la chiave pubblica genitore per ottenere la chiave pubblica figlia, senza mai conoscere la chiave privata.

Il funzionamento si basa sulla proprietà distributiva della moltiplicazione sulla curva ellittica. Sommare la chiave privata con un certo valore scalare e poi calcolarne

la chiave pubblica corrispondente equivale a sommare la chiave pubblica originale con lo stesso valore convertito in un punto sulla curva.

1.3 Sicurezza

Da un punto di vista più prettamente tecnico, la solidità di un HD wallet si basa innanzitutto sui presupposti della crittografia su curve ellittiche (ECC), per cui, data una chiave pubblica K, è computazionalmente impossibile ricavare la corrispondente chiave privata k senza risolvere il problema del **logaritmo discreto**.

Lo standard BIP 32 definisce specifiche proprietà di sicurezza:

- Data una chiave privata estesa figlia (k_i, c_i) e l'indice i, un attaccante non può risalire alla chiave privata del genitore k_{par} con un'efficienza superiore a un attacco di forza bruta su HMAC-SHA512 di 2^{256} operazioni.
- Dato un insieme di N coppie $(2 \leqslant N \leqslant 2^{32} - 1)$ di indice e chiave privata estesa $(i_j, (k_j, c_j))$, determinare se esse appartengano a una struttura gerarchica comune (ovvero se derivano dallo stesso genitore) non è computazionalmente più efficiente di un attacco di forza bruta su HMAC-SHA512 di 2^{256} operazioni.

Osserviamo che quest'ultima proprietà segue direttamente dall'effetto valanga caratteristico delle funzioni di hash: se il valore dell'indice varia, l'output di HMAC-SHA512 cambia in modo imprevedibile e, di conseguenza, la chiave figlia e il chain code corrispondente appariranno completamente casuali.

È tuttavia importante notare l'esistenza di alcuni potenziali pericoli:

- Data una chiave pubblica estesa del genitore (K_{par}, c_{par}) e una chiave pubblica figlia K_i, è possibile determinare il suo indice i attraverso una ricerca esaustiva.
- Data una chiave pubblica estesa del genitore (K_{par}, c_{par}) e una chiave privata figlia non hardened k_i, è possibile risalire alla chiave privata del genitore k_{par}.

Quest'ultimo fatto costituisce un rischio critico: una chiave privata figlia è calcolata come somma tra la chiave privata del genitore e il valore dell'output di HMAC, e questo può essere ricavato conoscendo la sola chiave pubblica estesa del genitore e il relativo chain code. Se un attaccante riuscisse a entrare in possesso della chiave pubblica estesa padre e, contemporaneamente, a ottenere anche una singola chiave privata figlia, potrebbe sottrarre il valore dell'output di HMAC dalla chiave figlia per risalire alla chiave privata estesa del genitore, ottenendo automaticamente tutte le chiavi dei livelli inferiori. La derivazione hardened previene questo problema.

Per queste ragioni, una chiave pubblica estesa deve essere custodita con maggiore attenzione rispetto alle normali chiavi pubbliche.

1.4 Codifica di chiavi estese

Affinché una chiave estesa possa essere facilmente trasmessa o importata tra diversi software, essa non viene gestita come dato grezzo, ma convertita in un indirizzo standardizzato. Prima della codifica finale, la chiave viene serializzata in una stringa di byte contenente, oltre alla chiave stessa, alcuni metadati utili a identificarne la posizione precisa all'interno dell'albero gerarchico.

La struttura serializzata ha una lunghezza fissa e comprende i seguenti campi:

1. **Versione** (4 byte): Ha la funzione di prefisso e determina come la chiave apparirà una volta codificata (per esempio "xprv" o "xpub"). Identifica anche la rete (*mainnet* o *testnet*) e lo standard di derivazione utilizzato.
2. **Profondità** (1 byte): Indica la profondità della chiave nell'albero di derivazione. Una chiave master ha profondità 0.
3. **Impronta del Genitore** (4 byte): È costituita dai primi 4 byte dell'hash HASH160 della chiave pubblica del genitore. Serve a identificare da quale nodo proviene la chiave corrente, facilitando la ricostruzione dell'albero, sebbene questo dato non sia strettamente necessario per la derivazione crittografica.
4. **Numero del Figlio** (4 byte): Rappresenta l'indice della chiave. La dimensione di questo campo (32 bit) è il motivo tecnico per cui un wallet non può generare più di 2^{32} figli per ogni livello.
5. **Chain Code** (32 byte): Contiene il chain code, che è indispensabile per la derivazione delle chiavi figlie.
6. **Chiave** (33 byte): Contiene la chiave vera e propria. Se si tratta di una chiave pubblica compressa, essa occupa nativamente 33 byte. Se si tratta di una chiave privata, che è di 32 byte, viene aggiunto un byte di *padding* `00` all'inizio per uniformare la lunghezza totale a 33 byte.

Una volta concatenati questi campi, al risultato viene aggiunto un ***checksum***, che consiste nei primi 4 byte del doppio hash SHA-256 dei dati serializzati, per prevenire errori di trascrizione.

Infine, l'intera sequenza viene codificata in **Base58**. Questo passaggio produce le stringhe leggibili che gli utenti sono abituati a vedere, come quelle che iniziano per `xprv` (*Extended Private Key*) o `xpub` (*Extended Public Key*).

2 Derivation Path

Un ***derivation path*** definisce la posizione esatta di una specifica chiave estesa (e dunque del relativo indirizzo) all'interno della struttura gerarchica di un HD wallet. Poiché le chiavi estese possono generare figli, e questi a loro volta altri figli, generalmente si ha a che fare con una struttura ad albero molto ramificata. Il percorso di derivazione è sostanzialmente la mappa che permette al wallet di navigare dalla chiave master fino a una specifica chiave figlia.

Per descrivere i percorsi di derivazione (derivation paths) si utilizza una notazione specifica. Si può subito notare come sembri ricalcare la notazione adottata per le directory dentro un file system:

- `m`: Rappresenta la chiave estesa master, derivata direttamente dal seed.
- /: Separa livelli successivi all'interno dell'albero.
- `'` o **h**: Indicano che la derivazione è hardened.

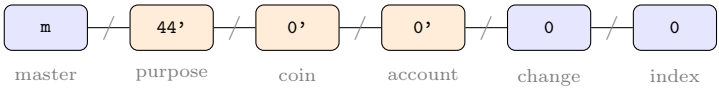


Fig. 3: Esempio di derivation path `m/44'/0'/0'/0/0` (BIP 44 Legacy). I nodi in arancione usano derivazione *hardened* (`'`).

Ad esempio, se si considera il percorso `m/1/2/3'`, questo identifica la chiave ottenuta seguendo questi passaggi:

1. Partenza dalla Master Key (`m`).
2. Derivazione (normale) del figlio con indice `1`.
3. Da questo, derivazione (normale) del figlio con indice `2`.
4. Da quest'ultimo, derivazione del quarto figlio hardened con indice `3'`.

Matematicamente, si è visto che gli indici *hardened* partono da 2^{31} (2.147.483.648). La notazione con l'apostrofo serve a semplificare la scrittura. Nell'esempio precedente, `3'` corrisponde all'indice reale 2.147.483.651, cioè $2^{31} + 3$.

2.1 Struttura del Wallet

Per garantire la compatibilità tra software diversi, è stato adottato uno standard che organizza l'albero delle chiavi seguendo cinque livelli logici fissi:

```
m / purpose' / coin_type' / account' / change / index
```

1. **Purpose**: Definisce lo schema adottato dal wallet usando il numero della BIP corrispondente. È sempre hardened.
2. **Coin Type**: Permette a un singolo seed di gestire più criptovalute diverse (`0'` corrisponde a Bitcoin). È sempre hardened.
3. **Account**: Permette di separare i fondi in diversi conti separati secondo le esigenze dell'utente. Il default è `0'`. È sempre hardened.

4. **Change**: Divide gli indirizzi in due categorie:
   - `0` definisce gli indirizzi di ricezione (esterni).
   - `1` definisce gli indirizzi di resto (interni, usati automaticamente dal wallet).
5. **Index**: È il contatore progressivo degli indirizzi.

Osserviamo che gli ultimi due livelli (Change e Index) sono derivazioni normali; pertanto, è possibile generare indirizzi a partire dalla chiave pubblica estesa dell'account corrispondente.

Al contrario, i livelli più interni prevedono la derivazione hardened, utilizzata di default essenzialmente per motivi di sicurezza. Come si è visto, infatti, un attaccante può facilmente entrare in possesso di una chiave privata estesa (e di tutti i suoi discendenti) conoscendo solamente la rispettiva chiave pubblica e una qualsiasi delle chiavi private figlie non hardened.

Per esempio, l'utilizzo di chiavi hardened a livello di account fa sì che l'eventuale compromissione di una chiave privata specifica non metta a rischio l'integrità della chiave master o degli altri account paralleli nella gerarchia.

2.2 Standard esistenti

I wallet moderni utilizzano percorsi diversi in base al tipo di indirizzo Bitcoin che devono generare. Ogni standard è descritto all'interno di una BIP, il cui numero è specificato all'interno del campo `Purpose` menzionato precedentemente.

Per quanto riguarda la codifica delle chiavi estese, la scelta della tipologia di indirizzo che si desidera utilizzare influisce sui byte di versione. Originariamente, lo standard definito da BIP 32 prevedeva l'uso dei prefissi "xprv" e "xpub" per distinguere chiavi private e pubbliche sulla mainnet e "tprv" e "tpub" per la testnet. Successivamente, con l'avvento di SegWit [4] e Taproot [17], molti sviluppatori pensarono di specificare il tipo di indirizzo adottato introducendo nuovi prefissi, come "yprv" e "ypub" o "zprv" e "zpub" [11].

BIP 44 [8]: Legacy

- **Percorso**: `m/44'/0'/0'/0/0`
- **Indirizzi**: P2PKH (iniziano con 1).
- **Prefisso**: `xprv` / `xpub`.

BIP 49 [13]: Nested SegWit

- **Percorso**: `m/49'/0'/0'/0/0`
- **Indirizzi**: P2SH-P2WPKH (iniziano con 3).
- **Prefisso**: `yprv` / `ypub` per distinguerle dalle legacy.

BIP 84 [10]: Native SegWit

- **Percorso**: `m/84'/0'/0'/0/0`
- **Indirizzi**: P2WPKH (iniziano con bc1q).
- **Prefisso**: `zprv` / `zpub`.

BIP 86 [15]: Taproot

- **Percorso**: `m/86'/0'/0'/0/0`
- **Indirizzi**: P2TR (iniziano con bc1p).
- **Prefisso**: `xprv` / `xpub`. Per evitare di creare ambiguità, vengono usati degli *output descriptors* [16].

Standard	Percorso	Indirizzi	Prefisso
BIP 44 [8], Legacy	`m/44'/0'/0'/0/0`	P2PKH (`1...`)	`xprv` / `xpub`
BIP 49 [13], Nested SegWit	`m/49'/0'/0'/0/0`	P2SH-P2WPKH (`3...`)	`yprv` / `ypub`
BIP 84 [10], Native SegWit	`m/84'/0'/0'/0/0`	P2WPKH (`bc1q...`)	`zprv` / `zpub`
BIP 86 [15], Taproot	`m/86'/0'/0'/0/0`	P2TR (`bc1p...`)	`xprv` / `xpub`*

Table 1: Standard di derivazione per i principali tipi di indirizzo Bitcoin. *Per evitare ambiguità con BIP 44, BIP 86 raccomanda l'uso di *output descriptors* [16].

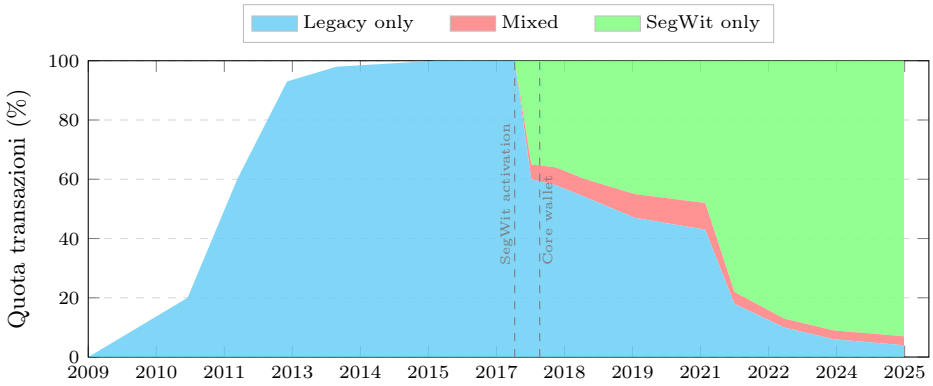


Fig. 4: Adozione di SegWit dal 2009 ad oggi: quota percentuale di transazioni legacy, miste e SegWit-only. Dati da `https://mainnet.observer/`.

3 Mnemonic seed

Come si è visto, un HD wallet è una tecnologia che semplifica drasticamente l'esperienza dell'utente, eliminando la necessità di backup frequenti. Il fatto che le chiavi non siano generate indipendentemente, ma bensì in maniera deterministica e gerarchica, riduce il problema della gestione del wallet a un unico punto cruciale: la memorizzazione e la custodia del seed, che consiste sostanzialmente in un numero molto grande.

Al fine di facilitare la gestione di questo dato per gli esseri umani, è stato introdotto un processo standard per associare a un seed la corrispondente ***seed phrase***, una sequenza di parole (solitamente 12 o 24) che può essere più facilmente gestita e ricordata.

3.1 Creazione della Mnemonica

La generazione di una frase mnemonica e del relativo seed segue un protocollo preciso, suddiviso logicamente in tre fasi distinte:

1. Generazione dell'entropia.
2. Conversione dell'entropia in mnemonica.
3. Derivazione del seed dalla mnemonica.

Generazione dell'Entropia Come prima cosa, è necessario generare dell'**entropia**, ovvero la sorgente di casualità raccolta dal sistema operativo, consistente in una lunga sequenza di bit. Al fine di garantire la sicurezza e la compatibilità con lo standard, l'entropia deve rispettare due requisiti principali:

- Deve essere compresa tra 128 e 256 bit.
- Deve essere un multiplo di 32 bit.

È fondamentale che, in questa fase, siano utilizzati **generatori di numeri casuali crittograficamente sicuri** per evitare prevedibilità nella creazione delle chiavi, in modo da non compromettere la sicurezza del wallet.

CSPRNG I generatori di numeri pseudo-casuali crittograficamente sicuri (CSPRNG, da *Cryptographically Secure Pseudo-Random Number Generator*) sono algoritmi progettati per produrre sequenze di bit computazionalmente indistinguibili da una distribuzione uniforme ideale.

Il funzionamento di un CSPRNG si basa sull'espansione deterministica di un valore segreto iniziale, detto *seed*, proveniente da una sorgente ad alta entropia. Una volta inizializzato, il generatore mantiene uno stato interno segreto che viene aggiornato iterativamente mediante primitive crittografiche a ogni nuova richiesta, permettendo così la generazione continua di sequenze pseudo-casuali [1].

Dal punto di vista della sicurezza, è fondamentale che l'eventuale compromissione dello stato interno attuale non consenta in alcun modo a un attaccante di dedurre i bit generati in passato, né di distinguerli da una sequenza puramente aleatoria (*backtracking resistance*). Analogamente, è indispensabile che la compromissione dello stato in un dato istante non pregiudichi l'imprevedibilità degli output futuri (*prediction resistance*). Si veda anche [2].

Le implementazioni standard si basano tipicamente sull'impiego di funzioni di hash, come SHA-256 o SHA-512, oppure su algoritmi di cifratura a blocchi, come AES in *counter mode* (CTR).

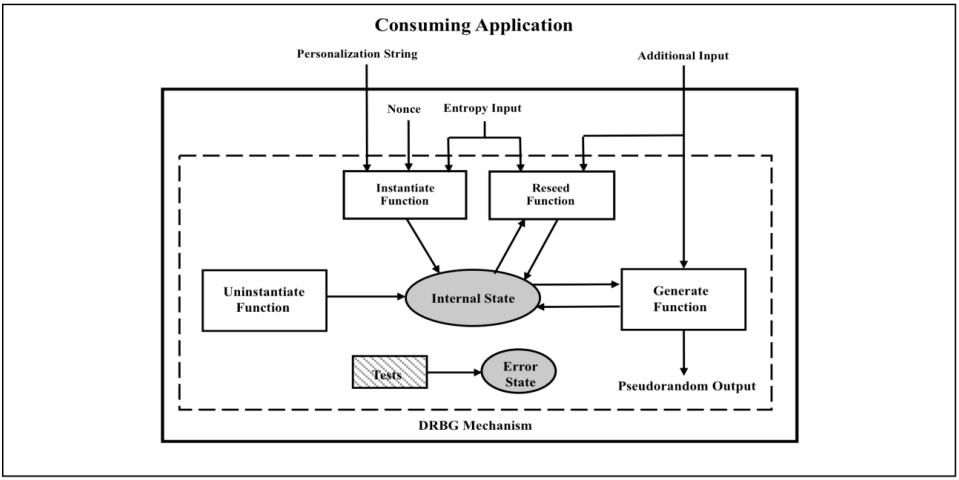


Fig. 5: Modello funzionale di un PRNG. Immagine tratta da [1].

Conversione nella Mnemonica Per rilevare eventuali errori di trascrizione futuri, viene innanzitutto aggiunto un checksum all'entropia, ottenuto calcolando l'hash **SHA-256** dell'entropia originale. Dal risultato dell'hash, viene prelevato 1 bit di checksum per ogni 32 bit di entropia. Ad esempio, per una stringa iniziale di 128 bit, il checksum è di 4 bit, mentre per 256 bit di entropia sono necessari 8 bit di checksum.

L'entropia originale viene poi concatenata con il checksum che è stato calcolato precedentemente. Il risultato totale è una sequenza di bit divisibile esattamente per 11, che viene quindi suddivisa in gruppi di 11 bit ciascuno.

Ciascun blocco viene convertito nel corrispondente numero decimale. Ora, 11 bit permettono di rappresentare valori numerici che vanno da 0 a 2047 (cioè $2^{11} - 1$), per cui ogni numero può essere considerato come un indice a cui associare una determinata parola, selezionata da una ***wordlist*** di 2048 termini inglesi, specificata all'interno di BIP 39 [9]. La sequenza di parole risultante costituisce la frase mnemonica (o seed phrase).

Per quanto è stato detto prima, la lunghezza della seed phrase non può essere arbitraria, poiché dipende dai bit di entropia utilizzati. Generalmente sono preferiti i formati da 12 o 24 parole, anche se non sono gli unici possibili.

La maggior parte dei wallet supporta esclusivamente la wordlist in lingua inglese, per cui è spesso sconsigliato l'uso di lingue diverse da questa per la creazione di una seed phrase.

La lista standardizzata da BIP 39 è stata progettata in modo da evitare ambiguità e semplificare la memorizzazione delle parole, secondo i seguenti criteri:

- **Selezione accurata delle parole**: è sufficiente digitare le prime quattro lettere di una parola per identificarla univocamente all'interno della lista;
- **Assenza di parole simili**, come ad esempio "*woman*" e "*women*", che, oltre a complicare la memorizzazione della frase, possono generare confusione ed errori;
- **Ordine alfabetico**, per facilitare la ricerca di una determinata parola all'interno della lista.

Calcolo del seed La frase mnemonica non è tuttavia utilizzabile direttamente dalla crittografia del wallet, per cui è necessaria la conversione in un **seed binario** di 512 bit (64 byte). Per questa operazione viene utilizzata la funzione PBKDF2 [2].

I parametri della funzione sono i seguenti:

- **Password**: La frase mnemonica stessa.
- **Sale**: La stringa costante "mnemonic" concatenata a una ***passphrase*** **opzionale** definita dall'utente.
- **Algoritmo**: HMAC-SHA512.
- **Iterazioni**: 2048.

Il risultato finale è un seed di 64 byte, che può essere usato per la generazione della chiave master di un HD wallet secondo lo standard definito da BIP 32.

La funzione PBKDF2 è progettata appositamente per essere lenta e macchinosa, attraverso le 2048 iterazioni di HMAC-SHA512, in modo da rendere difficile per un attaccante eseguire efficientemente attacchi di forza bruta per tentare di indovinare le frasi mnemoniche e derivare i seed corrispondenti.

[2] PBKDF2 (*Password-based Key Derivation Function 2*) [5] è un algoritmo crittografico standardizzato, utilizzato per derivare chiavi sicure dalle password minimizzando il rischio di attacchi di forza bruta.

ID	Word	ID	Word	ID	Word
0000	abandon	0038	age	0076	another
0001	ability	0039	agent	0077	answer
0002	able	0040	agree	0078	antenna
0003	about	0041	ahead	0079	antique
0004	above	0042	aim	0080	anxiety
0005	absent	0043	air	0081	any
0006	absorb	0044	airport	0082	apart
0007	abstract	0045	aisle	0083	apology
0008	absurd	0046	alarm	0084	appear
0009	abuse	0047	album	0085	apple
0010	access	0048	alcohol	0086	approve
0011	accident	0049	alert	0087	april
0012	account	0050	alien	0088	arch
0013	accuse	0051	all	0089	arctic
0014	achieve	0052	alley	0090	area
0015	acid	0053	allow	0091	arena
0016	acoustic	0054	almost	0092	argue
0017	acquire	0055	alone	0093	arm
0018	across	0056	alpha	0094	armed
0019	act	0057	already	0095	armor
0020	action	0058	also	0096	army
0021	actor	0059	alter	0097	around
0022	actress	0060	always	0098	arrange
0023	actual	0061	amateur	0099	arrest
0024	adapt	0062	amazing	0100	arrive
0025	add	0063	among	0101	arrow
0026	addict	0064	amount	0102	art
0027	address	0065	amused	0103	artefact
0028	adjust	0066	analyst	0104	artist
0029	admit	0067	anchor	0105	artwork
0030	adult	0068	ancient	0106	ask
0031	advance	0069	anger	0107	aspect
0032	advice	0070	angle	0108	assault
0033	aerobic	0071	angry	0109	asset
0034	affair	0072	animal	0110	assist
0035	afford	0073	ankle	0111	assume
0036	afraid	0074	announce	...	...
0037	again	0075	annual	2047	zoo

Table 2: Estratto della wordlist definita da BIP 39 [9]. La lista completa comprende 2048 termini inglesi, ciascuno identificato da un indice a 11 bit (da 0000 a 2047). Le parole sono state selezionate per essere univocamente identificabili dalle prime quattro lettere, prive di ambiguità visiva e ordinate alfabeticamente.

Osserviamo che la possibilità di usare una passphrase a discrezione dell'utente, in aggiunta alla mnemonica di partenza, fornisce un layer di sicurezza ulteriore, dal momento che questa altera l'output di PBKDF2 in maniera imprevedibile. In questo modo, anche se un attaccante venisse a conoscenza di tutte le parole che compongono la seed phrase, la sicurezza del wallet non sarebbe compromessa; per contro, l'arbitrarietà della passphrase costituisce una grande responsabilità per l'utente in termini di conservazione e gestione.

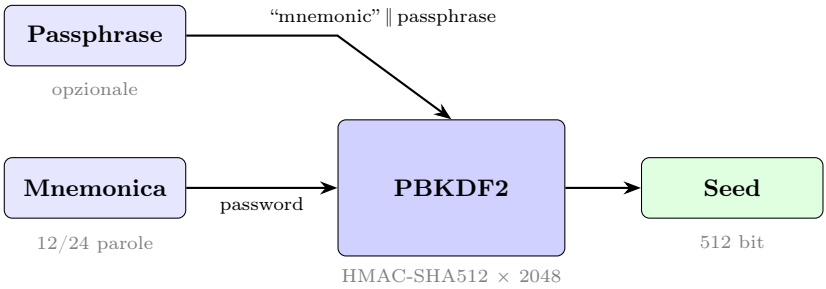


Fig. 6: Derivazione del seed tramite PBKDF2.

3.2 Validazione della Mnemonica

Per come è stato definito il processo di creazione, non è detto che una qualsiasi sequenza di parole costituisca una frase mnemonica valida. Grazie al meccanismo del checksum integrato, è possibile verificare matematicamente la validità di una frase.

Il processo di validazione inverte la creazione:

1. Le parole vengono convertite in bit.
2. Gli ultimi bit (quelli corrispondenti al checksum) vengono separati dal resto della stringa, contenente i bit effettivi di entropia.
3. Si ricalcola l'hash SHA-256 dell'entropia e si confronta il nuovo checksum con quello estratto dalla frase. Se i due coincidono, la frase è valida.

In altri termini, l'ultima parola della frase è necessariamente vincolata dalla scelta di quelle precedenti, poiché nella sua derivazione sono coinvolti i bit di checksum, univocamente determinati una volta generata l'entropia iniziale. Per questo motivo, è fortemente sconsigliato scegliere parole a caso dalla lista per creare un wallet, dal momento che, oltre al fatto che l'entropia generata sarà probabilmente molto bassa, è praticamente certo che l'ultima parola non sia matematicamente corretta, per cui la frase risulterà invalida.

References

1. Elaine Barker and John Kelsey. Recommendation for random number generation using deterministic random bit generators. Special Publication (SP) 800-90A Rev. 1, NIST, 2015.
2. L. Errati, R. La Scala, and M. Patano. Cryptographic standards for random number generation. In *CIFRIS25 ACTA*, volume 7 of *De Cifris Koine*, pages 217–223. De Cifris Press, September 2025. Leonardo Errati, 0009-0004-0460-9742; Roberto La Scala, 0000-0001-7468-0051; Mauro Patano, 0000-0003-1184-2062.

3. Hugo Krawczyk, Mihir Bellare, and Ran Canetti. HMAC: Keyed-hashing for message authentication. RFC 2104, IETF, 1997.
4. Eric Lombrozo, Johnson Lau, and Pieter Wuille. BIP 141: Segregated witness (consensus layer). Technical report, Bitcoin Improvement Proposal, 2015.
5. Kathleen Moriarty, Burt Kaliski, and Andreas Rusch. PKCS #5: Password-based cryptography specification version 2.1. RFC 8018, IETF, 2017.
6. National Institute of Standards and Technology. Secure hash standard (SHS). FIPS PUB 180-4, NIST, 2015.
7. National Institute of Standards and Technology. Digital signature standard (DSS). FIPS PUB 186-5, U.S. Department of Commerce, 2023.
8. Marek Palatinus and Pavol Rusnak. BIP 44: Multi-account hierarchy for deterministic wallets. Technical report, Bitcoin Improvement Proposal, 2014.
9. Marek Palatinus, Pavol Rusnak, Aaron Voisine, and Sean Bowe. BIP 39: Mnemonic code for generating deterministic keys. Technical report, Bitcoin Improvement Proposal, 2013.
10. Pavol Rusnak. BIP 84: Derivation scheme for P2WPKH based accounts. Technical report, Bitcoin Improvement Proposal, 2017.
11. SatoshiLabs. SLIP 132: Registered extended public key prefixes. Technical report, SatoshiLabs Improvement Proposal, 2017.
12. James M. Turner. The keyed-hash message authentication code (HMAC). *Federal Information Processing Standards Publication*, 198(1):1–13, 2008.
13. Daniel Weigl. BIP 49: Derivation scheme for P2WPKH-nested-in-P2SH based accounts. Technical report, Bitcoin Improvement Proposal, 2016.
14. Pieter Wuille. BIP 32: Hierarchical deterministic wallets. Technical report, Bitcoin Improvement Proposal, 2012.
15. Pieter Wuille. BIP 86: Deterministic wallet addresses for taproot. Technical report, Bitcoin Improvement Proposal, 2020.
16. Pieter Wuille and Andrew Chow. BIP 380: Output descriptors. Technical report, Bitcoin Improvement Proposal, 2021.
17. Pieter Wuille, Jonas Nick, and Anthony Towns. BIP 341: Taproot: Segwit v1 sigpubkey scripts. Technical report, Bitcoin Improvement Proposal, 2020.

zk-STARKs and Computational Integrity in Bitcoin Layer-2 Protocols

Bianca Rampazzo

BitPolito, Politecnico di Torino, Italy

Abstract. Zero-Knowledge proofs, such as zk-SNARKs, enable verification of computations without revealing private data. zk-STARKs are a type of SNARK: they are scalable, transparent, and post-quantum secure, making them particularly suited for blockchain applications. Bitcoin Script constraints prevent full on-chain verification, but Layer 2 protocols like Lightning and Ark can leverage STARKs to provide privacy-preserving, verifiable off-chain computations. BitVM2 introduces an interactive dispute mechanism to enforce correctness without modifying Bitcoin's base layer. The combination of STARKs and BitVM2 offers a scalable, secure, and post-quantum-resilient approach to enhancing Bitcoin through second-layer protocols.

Keywords: Bitcoin · Zero-Knowledge Proofs · STARKs · Consensus · Layer 2 · Lightning · Ark · BitVM2

1 Introduction

Bitcoin, introduced in 2009 as a peer-to-peer electronic cash system [6], relies on proof-of-work consensus to minimize trust among participants. While secure and decentralized [1], Bitcoin faces well-known challenges in scalability and privacy: each full node must verify all transactions, and on-chain data is publicly visible. These limitations motivate the use of cryptographic techniques to reduce verification costs and protect sensitive information.

Zero-Knowledge Proofs (ZKPs) allow one party to prove the correctness of a statement without revealing the underlying data. Among them, zk-STARKs offer scalability, transparency, and post-quantum security, relying solely on cryptographic

De Cifris Koine – BITCOIN & BLOCKCHAIN
https://doi.org/10.69091/koine/vol-6-B05

[1] Blockchain is a data structure consisting of a list of blocks securely linked together using cryptographic algorithms. The first widespread application emerged in 2009, after the advent of Bitcoin, and quickly proved to be one of the most disruptive technologies in recent years. Blockchains can be divided into three main categories: public permissionless (Bitcoin), private permissioned and public permissioned.

hash functions and requiring no trusted setup. This makes them particularly promising for blockchain applications where on-chain computation is constrained.

In Bitcoin, the UTXO (Unspent Transaction Output) model forms the backbone of transaction verification: every transaction consumes previous outputs and creates new ones, producing a graph of state transitions. While this stateless design simplifies validation, it imposes scalability limits as the global UTXO set must be maintained by all full nodes. Recent Layer 2 protocols, such as Lightning and Ark [2], extend the UTXO abstraction off-chain, enabling more efficient transaction execution while preserving Bitcoin's accounting logic. These off-chain structures are natural candidates for zero-knowledge proofs, as their state transitions can be succinctly represented and verified.

Direct verification of zk-STARKs on Bitcoin's base layer is infeasible due to block size constraints. Combining zk-STARKs with Layer 2 frameworks like BitVM2, which introduces interactive dispute mechanisms, enables scalable, privacy-preserving, and post-quantum-secure computation on Bitcoin without modifying its core protocol. The foundations of succinct arguments of knowledge and zero-knowledge proof systems have already been introduced in the context of blockchain technologies in Koiné Vol. 4 [4]. Building on that treatment, this work focuses specifically on transparent proof systems (zk-STARKs) and their potential applications within Bitcoin Layer 2 architectures.

2 Succinct Arguments and zk-SNARKs

For a broader introduction to succinct arguments of knowledge and their role in blockchain systems, the reader is referred to Koiné Vol. 4 [4]. Here we briefly recall the main definitions needed to discuss zk-STARKs and their applicability to Bitcoin.

Definition 1 *A **Succinct Non-interactive ARgument of Knowledge** (SNARK) is a triple of algorithms* $(\mathsf{S}, \mathsf{P}, \mathsf{V})$ *defined as follows:*

- $(\mathsf{pp}, \mathsf{vp}) \leftarrow \mathsf{S}(\mathcal{C}, \lambda, r)$*: a* setup algorithm *that, given a circuit* $\mathcal{C}$*, a security parameter* λ*, and some randomness* r*, generates a pair of public parameters:* pp *(prover parameters) and* vp *(verifier parameters).*
- $\pi \leftarrow \mathsf{P}(\mathsf{pp}, x, w)$*: a* proving algorithm *that, given the prover's parameters* pp*, a public input* x*, and a witness* w*, outputs a proof* π*. The proof must be of* sublinear size *with respect to the size of the witness.*
- $b \leftarrow \mathsf{V}(\mathsf{vp}, x, \pi)$*: a* verification algorithm *that, given the verifier's parameters* vp*, the public input* x*, and a proof* π*, outputs a bit* $b \in \{0, 1\}$*, where* 1 *indicates acceptance. The verifier must run in* sublinear time *with respect to the size of the circuit* $\mathcal{C}$*.*

[2] Transactions in Ark use virtual UTXOs, called VTXOs, which mimic Bitcoin's UTXO system but stay off-chain. When you send Bitcoin via Ark, you're actually creating a virtual transaction to the operator, who updates the VTXO records.

If the SNARK additionally satisfies the property of zero-knowledge (i.e., the proof π reveals no information about the witness w) then the scheme is referred to as a ***zero-knowledge SNARK*** *(zk-SNARK).*

Definition 2 *An argument system for circuit satisfiability is said to be* ***succinct*** *if it satisfies the following properties:*

- ***Proof length:*** *The total communication (i.e., the proof size ℓ_π) is sublinear in the size of the witness $|w|$, such as $\ell_\pi = \mathcal{O}(\log |w|)$. If $\ell_\pi = \mathcal{O}(\log |\mathcal{C}|)$, where $|\mathcal{C}|$ is the size of the circuit, the argument is said to be* strongly succinct.
- ***Verification time:*** *The time required by the verifier to check the proof is sublinear in the size of the circuit, for example* $\text{time}(\mathsf{V}) = \mathcal{O}(|x| + \log |\mathcal{C}|)$*, where $|x|$ is the size of the public input.*

Some definitions of succinctness only require the first condition (i.e., sublinear proof size), without imposing constraints on the verifier's runtime.

Before continuing, an informal definition of knowledge soundness is given to capture the extractor-based security intuition behind these proof systems.

Definition 3 *A non-interactive argument system for circuit satisfiability is said to be* ***adaptively knowledge sound*** *for a circuit $\mathcal{C}$ if the following holds:*

For any probabilistic polynomial-time (PPT) adversary $\mathcal{A}$ that outputs a proof π and public input x such that the verifier accepts with non-negligible probability κ, there exists a PPT extractor $\mathcal{E}$ (with black-box or non-black-box access to $\mathcal{A}$) that is able to extract a witness w such that:

$$\Pr[\mathcal{C}(x, w) = y] = \kappa - \varepsilon,$$

for some negligible function $\varepsilon(\lambda)$, where λ is the security parameter.

In this context, *adaptivity* means that the adversary is allowed to choose the statement x after observing the public parameters generated by the setup algorithm.

Knowledge soundness implies the standard notion of soundness. However, when the prover is computationally unbounded, the stronger property of knowledge soundness may not hold. In such a case, the argument system is referred to as a **SNARG** (Succinct Non-interactive ARgument), which guarantees only *soundness* rather than *knowledge soundness*.

2.1 Setup

When constructing a SNARK system, three main types of setup procedures can be distinguished:

- **Trusted setup per circuit:** In this approach, the setup phase generates random parameters specific to a particular circuit $\mathcal{C}$. It is crucial that the prover does not learn these secret random values; otherwise, they could forge proofs for false statements. This setup typically relies on a *trusted ceremony* to ensure the secrecy and integrity of the parameters.
- **Trusted but universal (updatable) setup:** The setup algorithm S is divided into two sub-algorithms:

$$\begin{cases} \text{Generate a universal reference string:} & gp \leftarrow S_{\text{init}}(\lambda, r), \\ \text{Derive circuit-specific parameters:} & (pp, vp) \leftarrow S_{\text{index}}(gp, C), \end{cases}$$

  where λ is the security parameter and r denotes randomness. In this setting, the random values generated in S_{init} are independent of the circuit C, allowing the setup to be reused across different circuits. Moreover, the universal parameters gp can be updated to improve security without restarting the entire setup.
- **Transparent setup:** the setup algorithm does not rely on any secret randomness. Instead, it uses only publicly verifiable procedures, such as cryptographic hash functions or publicly known constants, to generate the parameters. This approach removes the need for trust in the setup phase but often comes with increased computational costs.

There are two main paradigms for building SNARKs:

- **Functional commitment schemes combined with Interactive Oracle Proofs (IOPs):** this approach employs functional commitment schemes such as polynomial commitments, multilinear commitments, vector commitments, or inner product commitments, paired with compatible IOPs. The resulting constructions yield SNARKs that are applicable to general arithmetic circuits.
- **Pairing-based cryptography combined with linear Probabilistically Checkable Proofs (PCPs):** in this approach, SNARKs are constructed using bilinear pairings and are based on representations such as Quadratic Arithmetic Programs (QAPs). This method also supports general circuits and is notable for its succinctness and efficient verification.

While these formal definitions capture the cryptographic guarantees of succinct arguments, they do not yet explain why such systems are practically transformative. The missing conceptual bridge is computational integrity, introduced in Section 5: the ability to verify the correctness of arbitrary computations without re-executing them. zk-STARKs can be understood precisely as scalable realizations of this principle.

3 SNARKs outside Bitcoin

3.1 Ethereum: zkRollups and zkEVM

zkRollups are a layer 2 solution to solve scalability problems of Ethereum. Instead of sending all the transactions to the congested layer 1 network, we have a separate layer 2 network, which can be more centralized and with a much higher throughput. Layer 2 nodes will process all these transactions and compute a proof π that certifies their correctness. This increases by order of magnitude the number of transactions we can process per block, while maintaining the same security.

There are still difficulties in order to achieve zkRollups:

- We need to write very complicated arithmetic circuits, which are usually also of giant size
- There is no composability between different rollups. Different Layer 2 companies will build their own zkRollup, and this is an issue when, for example, we need to enable swaps (e.g. DeFi applications)

One idea is to build developer-friendly zero knowledge Ethereum Virtual Machine (zkEVM) that allows composability of different layer 2 network rollups.

zkEVM can prove that a batch of EVM transactions is valid using zero knowledge proofs. It's formed by a set of circuits, which can be used to prove that EVM is executing correctly. Unfortunately, it is notoriously hard to build and it has a large overhead. One of the difficulties is that there is a need to handle bytecode (such as OP codes). Luckily, the efficiency of SNARKs improved a lot recently. There are at least four different reasons that made zkEVM become very popular in the last 5 years:

1. We have different kind of setups because we have different kind of performing polynomial commitment schemes. Few years ago only Groth16 was considered practical for blockchain applications.
2. New arithmetization techniques such as CCS or Plonkish enable a lot more flexibility
3. Hardware acceleration
4. Recursive SNARKs, which further lower the cost of on-chain verification

Taken together, these advances have improved the practical efficiency of zkEVM systems by several factors compared with what was considered feasible only a few years ago.

zkEVM can be seen in three different flavors:

- Language level: instead of building ZKPs inside the existing Ethereum VM, build a totally new virtual machine, more friendly to SNARK computation. On top is a need of a compiler to compile EVM language like Solidity to the bytecode of the new virtual machine. Examples are: MatterLabs, Starkware.

- Bytecode level: directly check if the EVM bytecode was executed correctly. It can inherit the EVM execution model. It is possible to do some changes on how data are stored. As a tradeoff you get a longer prover time because many EVM primitives are not ZK-friendly. Examples are: Scroll, Hermez, Consensys.
- Consensus level: the idea is to maintain everything that Ethereum has (not only the execution level, but also the storage). Prover time is even higher and there is space for DDoS attacks. This idea is still under exploration. PSE (Privacy and Scaling Explorations, an Ethereum team) is exploring this possibility.

Although zkRollups were originally developed in the Ethereum ecosystem, their underlying principle (moving computation off-chain while keeping succinct verification on-chain) is blockchain-agnostic. The key question addressed in this work is whether a similar paradigm can be adapted to Bitcoin, despite its more restrictive execution model. To answer this, we must first formalize the properties and security guarantees of succinct arguments of knowledge.

3.2 Monero: Ring Confidential Transactions (RingCT)

Confidential transactions aim to provide strong financial privacy while preserving the public verifiability that characterizes blockchain systems. In a traditional blockchain such as Bitcoin, transaction metadata (including sender, receiver, and transferred amount) are publicly visible by design, ensuring transparency and auditability. Large-scale data analysis techniques can sometimes reconstruct transaction graphs or infer relationships between users. Confidential transaction systems address the inherent trade-off between transparency and privacy by concealing sensitive transaction data while still allowing the network to verify fundamental correctness properties, such as conservation of value and authorization of spending. In this sense, they attempt to reconcile privacy with cryptographic accountability.

Monero adopts an approach based on layered cryptographic obfuscation techniques integrated directly into transaction construction. Privacy is mandatory by design: every transaction benefits from the same anonymity guarantees.

At the core of Monero's model are **ring signatures**. When a user spends an output, the signature proves that one element in a set of possible inputs is authorized to spend funds, without revealing which one. This mechanism provides sender ambiguity, as observers cannot determine which member of the ring corresponds to the actual spender.

Receiver privacy is achieved through **stealth addresses**. Instead of publishing a reusable address, the recipient's public key is used to derive a unique one-time destination for each transaction. Only the intended recipient can recognize and spend the output, while external observers cannot link multiple payments to the same user.

To conceal transaction amounts, Monero employs **Pedersen commitments** [3]. These commitments hide numerical values while preserving additive homomorphism, allowing the network to verify that inputs equal outputs without revealing the underlying amounts.

Finally, **Bulletproofs** are used to prove that committed values lie within a valid range (e.g., non-negative and below a fixed upper bound). This prevents overflow attacks and ensures monetary soundness, while keeping proofs relatively compact compared to earlier range proof constructions.

Monero's architecture therefore relies on multiple cryptographic primitives (ring signatures, commitments, and range proofs) each contributing a specific privacy property. The system achieves strong anonymity, but at the cost of increased transaction size and verification overhead.

3.3 Zcash: zk-SNARK-Based Privacy

Zcash follows a different paradigm: instead of embedding obfuscation directly into transaction structure, it relies on succinct zero-knowledge proofs to enforce correctness without revealing data.

Zcash uses zk-SNARKs, specifically pairing-based constructions such as Groth16 [4], to enable **shielded transactions**. A shielded transaction hides the sender, receiver, and transferred amount simultaneously, while still proving that the transaction satisfies all consensus rules.

Unlike Monero, privacy in Zcash is optional. The protocol supports two types of addresses:

- **t-addresses** (transparent), which function similarly to Bitcoin addresses.
- **z-addresses** (shielded), which enable zero-knowledge privacy.

This dual design allows interoperability with transparent systems, but also introduces complexity, as transactions may move between transparent and shielded pools.

How zk-SNARKs Are Used in Zcash

In Zcash, a zk-SNARK proof attests that a transaction is valid without revealing its private inputs. More precisely, the prover demonstrates knowledge of secret data satisfying a set of arithmetic constraints that encode transaction rules.

These constraints ensure:

[3] Pedersen commitments rely on the hardness of the discrete logarithm problem and provide additive homomorphism, a property that is essential for balance verification.

[4] These constructions are based on bilinear pairings over elliptic curves and enable extremely short proofs and efficient verification. See Koiné Vol. 4 [4].

- *Conservation of value:* no coins are created or destroyed.
- *No double spending:* previously spent notes cannot be reused.
- *Authorization:* the spender possesses the correct secret key.

All of these properties are enforced while keeping the transaction's inputs, outputs, and amounts confidential. Verification is efficient: the proof is succinct (typically a few hundred bytes) and can be checked quickly by all nodes.

The introduction of the Sapling protocol significantly improved the performance of shielded transactions. It reduced proving time and memory requirements, making privacy more practical for end users. However, the system still relies on a trusted setup ceremony to generate common reference parameters. Although carefully engineered to minimize trust assumptions, this requirement represents a structural difference from transparent blockchain designs.

3.4 Design Trade-offs: Obfuscation vs Succinct Proofs

Monero and Zcash illustrate two contrasting approaches to blockchain privacy.

Monero distributes privacy across multiple cryptographic components embedded in transaction format. Privacy is mandatory and uniform across the network, but transaction sizes and verification costs are comparatively higher.

Zcash, by contrast, encapsulates privacy inside a succinct proof system. The blockchain verifies only a compact proof attesting to transaction validity, rather than inspecting the transaction data itself. This leads to smaller on-chain footprints but introduces reliance on advanced cryptographic assumptions and trusted setup procedures.

Both systems require protocol-level modifications and depart significantly from Bitcoin's minimalist design philosophy. They demonstrate that strong privacy guarantees are achievable, but only through substantial cryptographic integration into consensus.

Bitcoin, in contrast, has historically prioritized conservative evolution and minimal script complexity. This raises a fundamental question: can advanced zero-knowledge systems, particularly transparent and post-quantum constructions such as zk-STARKs, enhance Bitcoin without altering its core consensus rules?

4 Foundations of zk-STARKs

At the heart of STARKs lies the concept of **IOPs** (Interactive Oracle Proofs): an extension of traditional interactive proofs where the verifier can query the prover's messages like an oracle. This setup enables efficient verification of large objects, such as polynomials, by combining probabilistic checks with algebraic encodings. To bridge the gap between general computation and algebra, STARKs rely on **arithmetization**. A common framework is the Algebraic Intermediate

Representation (**AIR**), where computations are expressed as sequences of states organized in a trace table, and transition constraints ensure correct evolution. An alternative approach is Customizable Constraint Systems (CCS), which also encode computation into polynomial relations. In this framework, a computation is captured as a trace polynomial, and constraints are aggregated into a composition polynomial, reducing verification to probabilistic polynomial identity testing. The soundness of this process is guaranteed by the Fast Reed–Solomon IOP of Proximity (**FRI**), which efficiently checks closeness to low-degree polynomials in logarithmic rounds, achieving security with minimal cryptographic assumptions, relying primarily on hash commitments. From a mathematical perspective, STARKs rely on finite-field arithmetic, low-degree polynomial testing, Reed–Solomon error-correcting codes, Merkle-tree commitments, and the Fiat–Shamir heuristic to obtain non-interactive proofs.

Protocol Overview

A zk-STARK proof proceeds as follows:

1. The prover constructs a trace of the computation.
2. The trace is encoded as polynomials over a finite field. [5]
3. The prover commits to these polynomials via Merkle trees.
4. Using FRI, the prover shows proximity to low-degree polynomials.
5. The verifier queries a few positions and checks consistency.

The result is a succinct proof: large computations reduce to proofs that are logarithmic in size and verifiable in milliseconds.

Note: *the term "SNARK" is often misused. It is frequently restricted to SNARKs that require a trusted setup (e.g., Groth16), but it properly encompasses setup-free protocols such as STARKs. Similarly, "STARK" is sometimes used to refer specifically to StarkWare's implementation, rather than the broader class of transparent, setup-free SNARKs. Moreover, although STARKs are sometimes described as interactive, real-world deployments are typically non-interactive.*

5 Computational Integrity with ZK-STARKs

The motivation behind STARKs lies in the concept of computational integrity: the guarantee that the result of a computation is correct without having to re-execute it. This principle is crucial because it shifts the computational burden from the verifier to the prover, making it possible to validate processes that would otherwise require enormous amounts of time and resources. Computational integrity forms

[5] In practice, the prover works over large finite fields and represents the computation through polynomial constraint systems whose consistency is verified probabilistically.

the foundation of many practical applications, such as blockchain systems, where trust cannot be delegated to a central authority but must instead emerge from the transparency and efficiency of cryptographic protocols. In this context, STARKs present themselves as a scalable and secure solution, capable of proving the correct execution of arbitrary programs while ensuring transparency and resistance against future adversaries equipped with quantum computers.

5.1 The DNA Profile Match Example

A motivating example of the problem addressed by [2] is the DNA Profile Match (DPM) scenario. Suppose a national police force (P), which maintains a confidential forensic DNA profile database (D), claims that the DNA profile (p) of a controversial presidential candidate does not appear in D. How can cryptographic protocols be used to convince the skeptical public of this claim, without revealing any information about D or p, without relying on any trusted third party, and within reasonable computational effort?

This illustrates a broader issue: when a party P performs a computation C on a dataset D, there is a risk that P might misreport the result $C(\mathrm{D})$, thereby undermining computational integrity (CI). If the dataset D is public, a verifier V can recompute C on D and compare the result, but this is inefficient. If D contains private data, verification risks exposing sensitive information. Traditionally, one would resort to a trusted auditor, but this introduces centralization and scalability limits. Zero-knowledge proof systems offer a compelling alternative.

5.2 Zero-knowledge proofs

A zero-knowledge proof system for a computation C consists of a prover P and a verifier V. The prover convinces the verifier that a computation was correctly executed without revealing additional information. A secure ZK system satisfies:

- **Completeness:** an honest prover can convince the verifier of a true statement.
- **Soundness:** a dishonest prover cannot convince the verifier of a false statement, except with negligible probability.

Early ZK systems with scalable verification were based on **Probabilistically Checkable Proofs (PCPs)**, which established that:

1. The prover's runtime is polynomial in the computation: $T_P = T_C^{O(1)}$
2. The verifier's runtime is polylogarithmic: $T_V = \log^{O(1)} T_C$

These constructions introduced three essential properties: post-quantum security (hash-based, no trusted setup), succinct arguments of knowledge (demonstrating

knowledge without revealing it), and transparency. In particular, ZK-STARKs stand for Zero-Knowledge Scalable Transparent Arguments of Knowledge, where the prover must prove knowledge of information without revealing it. For our example (Sec. 5.1), the police need to prove that the politician's DNA profile does not appear in their database, without revealing the database content D or the profile p itself.

5.3 Trade-offs: Prover vs. Verifier

The efficiency profile of STARKs is asymmetric:

- **Prover:** Proof generation can be resource-intensive, requiring hours and large memory (terabytes in experiments).
- **Verifier:** Verification is lightweight, requiring kilobytes of data and milliseconds of computation.

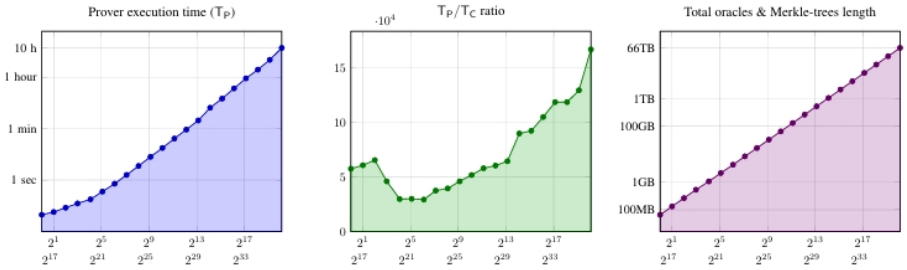


Fig. 1: Prover running time (left, log–log scale) as a function of the number of entries n in the DNA profile database; ratio of proving time to naïve execution time (centre, log scale on the horizontal axis); total size of oracles and Merkle commitment trees generated during execution (right, log–log scale).

6 SNARKs in Bitcoin

The asymmetric efficiency profile of zk-STARKs (computationally heavy proving and lightweight verification) appears, at first glance, well aligned with blockchain architectures. In decentralized systems, a limited number of actors may generate proofs, while thousands of nodes verify them. This suggests that succinct proof systems could enhance scalability without compromising decentralization. However, any attempt to integrate zero-knowledge verification directly into Bitcoin must confront the severe constraints imposed by Bitcoin Script.

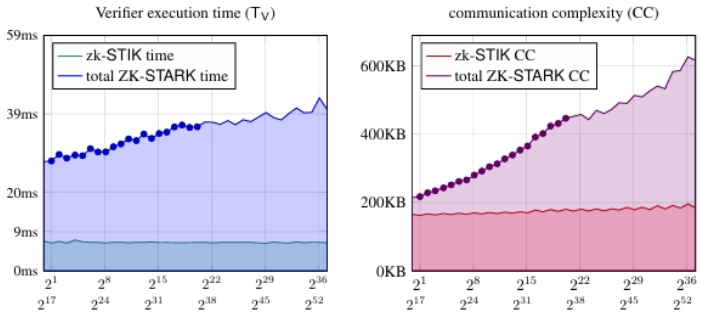


Fig. 2: Verifier running time (left) and communication complexity (right) as a function of n; horizontal axis logarithmic, vertical axis linear. The lower line shows the ZK-STARK verifier complexity, the upper line the naïve verifier.

6.1 Bitcoin's Execution Model

Bitcoin Script was deliberately designed as a minimal, non-Turing-complete language. Its restricted expressiveness prioritizes security, determinism, and predictable validation costs over computational flexibility. Standard scripts are subject to strict limits on size, stack depth, and arithmetic operations. In particular:

- Arithmetic is limited to small integers.
- There is no native support for multi-precision field arithmetic.
- Essential operations for modern cryptographic verifiers, such as efficient concatenation (`OP_CAT`) or wide-field multiplication, are absent.

Moreover, every script is executed by all validating nodes. Consensus therefore imposes strong constraints on execution time and memory usage. Any complex verification logic embedded at Layer 1 would directly increase the validation burden on the entire network.

These structural characteristics fundamentally restrict the feasibility of deploying modern zero-knowledge verifiers inside Bitcoin consensus.

6.2 SNARKs vs STARKs on Layer 1

The limitations affect zk-SNARKs and zk-STARKs differently.

zk-SNARKs offer extremely compact proofs and efficient verifiers. For example, pairing-based systems such as Groth16 produce proofs of only a few hundred bytes. In principle, this compactness makes them attractive candidates for on-chain verification.

However, Bitcoin Script does not support pairing-based cryptography. Emulating elliptic curve pairings inside Script would require thousands of opcodes and intricate constructions that approach or exceed standard limits. Furthermore, many SNARK systems rely on trusted setup ceremonies, which conflict with Bitcoin's conservative trust model.

zk-STARKs eliminate trusted setup and provide post-quantum security, aligning better with Bitcoin's long-term security philosophy. Yet these advantages come at a cost: significantly larger proofs and hash-intensive verification procedures. A typical STARK verifier performs numerous Merkle path checks and polynomial evaluations, requiring thousands of hash computations and nontrivial finite-field arithmetic.

Such requirements exceed Bitcoin Script's practical capabilities. Script size limits, stack constraints, and the absence of native wide-field arithmetic render full STARK verification infeasible under current consensus rules.

6.3 Implications

The conclusion is not merely that on-chain verification is inefficient, but that Bitcoin Layer 1 is structurally incompatible with sophisticated zero-knowledge verification under its current design.

This observation does not undermine the value of zk-STARKs. Rather, it clarifies where their integration is most natural. If Layer 1 must remain minimal and conservative, then computationally intensive cryptographic mechanisms should be deployed outside consensus, with only minimal commitments anchored on-chain.

This design philosophy leads directly to Layer 2 constructions, where computation is moved off-chain while Bitcoin provides final settlement and security guarantees.

7 Layer 2 Applications

In Layer 2, STARKs provide recurring benefits: privacy, compact proofs, and operator accountability. These apply differently in specific systems.

7.1 Lightning Network

The Lightning Network is Bitcoin's most widely deployed Layer 2 protocol [7]. It enables fast, low-fee payments but struggles with privacy and verifiability. STARKs could potentially address these challenges:

- **Privacy:** Channel balances and routing correctness can be proven without revealing sensitive details.
- **Verifiability:** Instead of replaying the entire history of a channel, nodes could verify a compact proof of the final state.

7.2 Ark Protocol

Ark is a new experimental Layer 2 proposal based on Virtual UTXOs (VTXOs) [3]. An operator batches off-chain transactions into on-chain commitments and prevents double-spending. Transactions use VTXOs, which mimic Bitcoin's UTXO system but remain off-chain. Unlike Bitcoin, this isn't peer-to-peer; it's more like a client-server model, with the operator keeping track of balances.

STARKs could strengthen Ark by:

- Providing proofs of inclusion/exclusion for VTXOs without revealing details.
- Enabling privacy-preserving transaction batching.
- Allowing succinct client-side verification.
- Enforcing operator accountability.

Though experimental, Ark highlights how zk-STARKs could enhance trust-minimized scalability beyond Lightning.

8 Bridging Bitcoin to Second Layers via BitVM2

Recent proposals suggest that Bitcoin may still support advanced off-chain computation verification without modifying its base-layer rules. One of the most notable approaches is BitVM [1] and its evolution, BitVM2 [5].

BitVM, originally proposed as a theoretical framework for expressing arbitrary computations through Bitcoin Script using optimistic verification, demonstrates that complex programs can be enforced on Bitcoin without changing consensus. The core idea is not to verify an entire computation on-chain, but to enable a challenge-response mechanism in which incorrect execution can be disputed.

BitVM2 refines this model by improving efficiency, modularity, and practical deployability. Instead of requiring full on-chain verification of a zero-knowledge proof, BitVM2 enables interactive fraud proofs. In this model, a prover claims that a certain computation has been executed correctly off-chain. If no challenge is raised, the claim stands. If a challenger disputes the claim, the protocol reduces the disagreement to a minimal computational step that can be verified using existing Bitcoin Script primitives.

This approach is fundamentally different from zk-STARK verification. Rather than relying on succinct non-interactive proofs, BitVM2 adopts an optimistic paradigm:

- Computation is performed off-chain.
- A commitment to the result is posted on-chain.
- Verification occurs only in the presence of disputes.

The relevance of BitVM2 to zk-STARK-based systems lies in hybrid constructions. Instead of verifying an entire STARK proof on-chain, Bitcoin could enforce the correctness of a STARK verifier through an interactive dispute game. In such a design: a prover generates a STARK proof off-chain and the proof verification logic is executed off-chain. If challenged, the disagreement is reduced to a specific verification step, which can be checked via BitVM2's interactive mechanism.

This significantly reduces the on-chain computational burden, while preserving strong correctness guarantees under an **honest-challenger assumption**.

From a systems perspective, BitVM2 provides a missing architectural bridge between Bitcoin's conservative Layer 1 and advanced cryptographic constructions deployed at Layer 2. It allows Bitcoin to remain minimal and deterministic, while still anchoring arbitrarily complex off-chain computations.

In the context of Layer 2 systems such as Lightning or Ark, BitVM2 could enhance operator accountability. For example:

- A Lightning channel factory could commit to off-chain state transitions, with disputes resolved via BitVM2.
- An Ark operator could be required to prove correct batching of VTXOs, with fraud proofs enforced on-chain.

Thus, BitVM2 does not replace zk-STARKs, but complements them. While STARKs provide scalable and transparent proofs of computation, BitVM2 provides a mechanism for enforcing computational correctness within Bitcoin's existing execution constraints.

This architecture aligns with Bitcoin's conservative philosophy while enabling expressive second-layer systems. Rather than modifying consensus to accommodate advanced cryptography, the system leverages economic incentives and dispute resolution to preserve security.

9 Conclusion

zk-STARKs provide a powerful framework for achieving computational integrity, privacy, and post-quantum security in blockchain systems. While Bitcoin's Layer 1 consensus imposes strict limits that make on-chain verification of full STARK proofs impractical, Layer 2 protocols offer fertile ground for their deployment. Lightning and Ark illustrate how STARKs enable compact verification, enhanced privacy, and operator accountability. BitVM2 complements this approach by providing an interactive, dispute-based mechanism that allows Bitcoin to enforce the correctness of complex off-chain computations without modifying the base-layer consensus. By combining STARK-based proof generation with BitVM2's optimistic verification, off-chain computations can be anchored securely on-chain, disputes resolved efficiently, and decentralization preserved. Together, these tools outline a layered verification

architecture: heavy computation occurs off-chain, succinct or interactive commitments anchor results on-chain, and disputes are resolved within Bitcoin Script's existing capabilities. This hybrid model demonstrates that advanced cryptography can extend Bitcoin's functionality safely, maintaining minimalism at Layer 1 while enabling expressive, scalable, and privacy-preserving Layer 2 systems.
More broadly, these developments illustrate how transparent proof systems can complement Bitcoin's conservative design philosophy, extending functionality without requiring modifications to the underlying consensus protocol.

References

1. Lukas Aumayr, Zeta Avarikioti, Robin Linus, Matteo Maffei, Andrea Pelosi, Clara Stefo, and Alexei Zamyatin. BitVM: Quasi-turing complete computation on bitcoin. Technical Report Report 2024/1995, IACR Cryptology ePrint Archive, 2024.
2. Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev. Scalable, transparent, and post-quantum secure computational integrity. IACR Cryptology ePrint Archive, Report 2018/046, 2018.
3. Bitcoin Ops. Ark documentation, 2023. Topic overview.
4. M. Kohlweiss and A. Nitulescu. Snarks. In *Advanced Cryptographic Protocols*, volume 4 of *De Cifris Koine*, pages 45–71. De Cifris Press, October 2024. Markulf Kohlweiss, 0000-0002-8660-9663; Anca Nitulescu, 0000-0001-9149-2036.
5. Robin Linus, Lukas Aumayr, Andrea Pelosi, Zeta Avarikioti, Matteo Maffei, and Alexei Zamyatin. BitVM2: Bridging bitcoin to second layers, 2024.
6. Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008. Self-published.
7. Joseph Poon and Thaddeus Dryja. The bitcoin lightning network: Scalable off-chain instant payments, 2016. Draft paper.

Attacco ad un sottogruppo di chiavi del sistema Bitcoin

Domenica Sogiorno

domenicasogiorno@gmail.com

Abstract. Il protocollo di generazione degli indirizzi Bitcoin è sicuro? Ce lo siamo chiesti e abbiamo provato a generare indirizzi BTC partendo da uno speciale sottogruppo del gruppo delle chiavi private. Il risultato, che vi invitiamo a leggere nell'articolo, ci fa concludere che è fondamentale, per la sicurezza del sistema, che le chiavi private vengano scelte in maniera casuale. Di tale approccio, dati i risultati, non vi è certezza.

1 Introduzione

Il sistema Bitcoin [6] è stata la prima applicazione della tecnologia blockchain, letteralmente *"catena di blocchi"*, nonché un sistema di registro digitale immutabile utilizzato in reti distribuite, prive di autorità centrali. In breve, tale sistema consente ad una comunità di utenti di scambiarsi risorse digitali attraverso la pubblicazione di transazioni in un registro pubblico immutabile. L'introduzione dell'idea alla base della tecnologia blockchain risale al 1991, però è stato dal 2008 in poi che tale tecnologia è stata usata per la prima volta nel sistema **Bitcoin** proprio perché risultava adatta al sistema nascente: la moneta elettronica è protetta solo da meccanismi di crittografia, la rete è totalmente decentralizzata non essendoci terze parti che intervengono nella gestione della stessa e peer-to-peer poiché nessun utente ha privilegi sugli altri e ciascuno di essi può contribuire alla funzione del sistema interno.

Ogni nodo (nonché utente del sistema) ha bisogno di un account che lo identifichi all'interno della comunità/della rete. Si può pensare a questo come all'account di una banca; al posto di nome utente e password, però, si hanno rispettivamente chiave pubblica e chiave privata. Entrambe le chiavi sono sequenze alfanumeriche; la chiave privata è usualmente generata in maniera random da una funzione sicura scelta opportunamente e la chiave pubblica è generata da questa tramite un algoritmo scelto dal sistema BTC.

La robustezza di un crittosistema risiede nell'impossibilità computazionale della derivazione delle chiavi private dai dati pubblici. In Bitcoin, tale sicurezza è garantita

De Cifris Koine – BITCOIN & BLOCKCHAIN
https://doi.org/10.69091/koine/vol-6-B06

dalla complessità del problema del logaritmo discreto per curve ellittiche (ECDLP: Elliptic Curve Discrete Logarithm Problem) e dall'integrità delle funzioni crittografiche correlate. Tuttavia un'eventuale distribuzione non uniforme delle chiavi potrebbe restringere drasticamente lo spazio di ricerca, esponendo il sistema a vulnerabilità.

Nel 2018, durante un'attività di ricerca svoltasi in un periodo di stage presso l'Università degli Studi di Trento sotto la supervisione dei Prof. Massimiliano Sala (UNITN) e Roberto La Scala (UNIBA), in collaborazione con il Dott. Daniele Taufer, è stata esplorata l'ipotesi che alcune chiavi crittografiche potessero trovarsi in sottogruppi limitati e ispezionabili. Nonostante le comuni previsioni statistiche suggerissero il contrario, l'analisi di queste porzioni ridotte dello spazio delle chiavi ha rivelato la presenza di indirizzi attivi. Tale riscontro ha reso prioritario lo sviluppo di un protocollo di notifica volto a informare e proteggere i proprietari dei fondi potenzialmente esposti.

Quanto qui esposto è già stato oggetto di un approfondimento nell'articolo pubblicato il 24 settembre 2020.[7]

Il presente contributo si articola come segue: la sezione 2 richiama i fondamenti matematici necessari per la comprensione dei concetti successivi; la sezione 3 illustra il funzionamento del sistema BTC e il relativo algoritmo di generazione degli indirizzi; infine, l'ultima sezione presenta il progetto di ricerca sviluppato e i risultati conseguiti.

2 Richiami teorici

2.1 Funzioni hash

Definizione 1 *Una funzione hash è una funzione matematica che prende in input una stringa di bit di lunghezza arbitraria e restituisce in output una stringa di lunghezza fissa, chiamata* digest*.*

Le funzioni hash risultano essenziali per garantire l'integrità dei dati; esse producono un'impronta digitale univoca di un documento, permettendo di verificarne l'autenticità e l'assenza di alterazioni.
Una funzione hash per essere considerata sicura, deve essere tale da rendere i tre problemi seguenti difficili da risolvere:

Problema 1 **"Collision"**: data una funzione hash $h : X \to Y$ trovare $x, x' \in X$, $x \neq x'$, tali che $h(x) = h(x')$.
Una funzione hash per la quale il problema della collisione non può essere risolto in maniera efficiente è chiamata "collision resistant".

Problema 2 **"Preimage"**: data una funzione hash $h : X \to Y$ e dato $y \in Y$

trovare $x \in X$ tale che $h(x) = y$.
Una funzione hash per la quale il problema della preimage non può essere risolto in maniera efficiente è chiamata "preimage resistant" o funzione "one-way".

Problema 3 **"Second Preimage"**: data una funzione hash $h : X \to Y$ e dato $x \in X$ trovare $x' \in X$, $x \neq x'$, tale che $h(x) = h(x')$.
Una funzione hash per la quale il problema della second preimage non può essere risolto in maniera efficiente è chiamata "second preimage resistant".

Dunque una funzione hash si considera **sicura** se essa ha le tre proprietà precedenti, cioè è collision resistant, preimage resistant e second preimage resistant [9].

2.2 Curve ellittiche

Definizione 2 ([10]) *Si consideri K un campo di caratteristica diversa da 2 e da 3 e un polinomio di terzo grado $x^3 + ax + b$ $(a, b \in K)$ che abbia radici tutte distinte. Si definisce curva ellittica non singolare l'insieme*

$$E = \{(x, y) \in K \times K \mid y^2 = x^3 + ax + b,\ a, b \in K\} \bigcup \{\mathcal{O}\}$$

cioè l'insieme delle soluzioni $(x, y) \in K \times K$ dell'equazione $y^2 = x^3 + ax + b$ più un punto speciale chiamato punto all'infinito $\mathcal{O}$.

In questa sezione ci occupiamo di curve non singolari; tali curve hanno la proprietà secondo cui preso un qualsiasi punto su esse esiste la tangente alla curva per il punto.

Data E una curva ellittica non singolare, si definisce su essa un'operazione binaria che rende E un gruppo abeliano. Introduciamo, per semplicità, la definizione nel caso $K = \mathbb{R}$, che fa riferimento alla rappresentazione geometrica della curva nel piano.

Definizione 3 *Sia E una curva ellittica non singolare su $\mathbb{R}$, allora si definisce l'operazione*

$$+ : E \times E \to E$$

che ad una coppia di punti della curva ne associa un terzo seguendo le seguenti regole. Dati $A = (x_1, y_1)$, $B = (x_2, y_2) \in E$ allora:

1. *se $x_1 \neq x_2$:*
   si considera la linea congiungente i due punti A e B, che interseccherà la curva in un terzo punto C. Si definisce somma di A e B il punto R, simmetrico di C rispetto all'asse x.

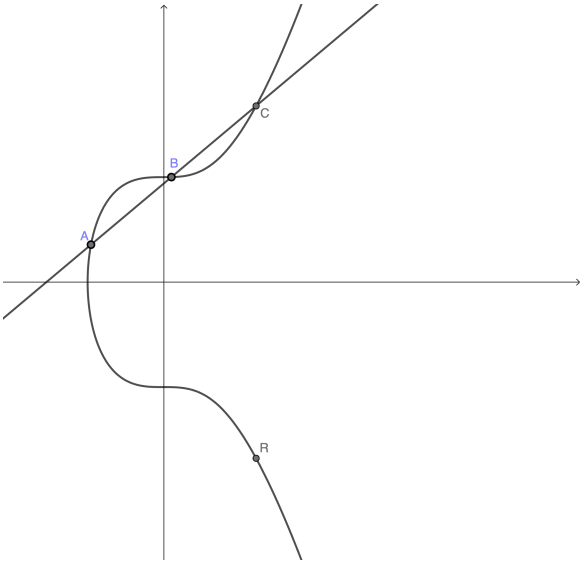


Fig. 1: Curva non singolare $y^2 = x^3 + 7$ definita su $\mathbb{R}$

2. *se* $x_1 = x_2$ *e* $y_1 = -y_2$*:*
   la linea congiungente i due punti non interseca la curva in punti diversi da A *e* B*; si assume allora che la intersechi all'infinito e dunque* $A + B = \mathcal{O}$*, cioè* A *è l'opposto di* B*.*

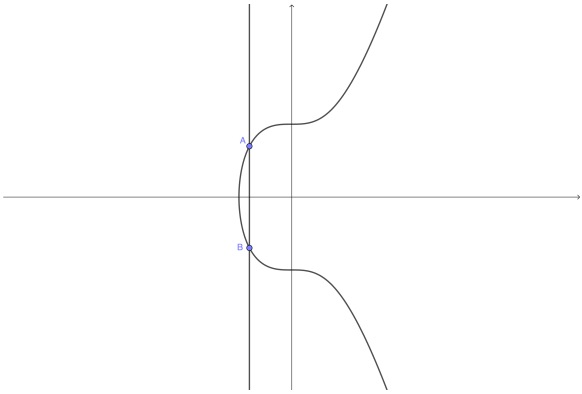


Fig. 2: Curva non singolare $y^2 = x^3 + 7$ definita su $\mathbb{R}$

3. *se $x_1 = x_2$ e $y_1 = y_2$, cioè A e B coincidono:*
   si considera la linea tangente la curva passante per il punto. Detto C l'altro punto in cui la retta interseca la curva ellittica, si definisce $2A = R$ con R simmetrico di C rispetto all'asse x.
   Questo caso comprende uno più particolare, cioè quello per cui i punti coincidono e il punto è sull'asse x. La retta tangente alla curva passante per il punto in questione non interseca la stessa in altri punti; per cui si assume $2A = \mathcal{O}$ cioè A è l'opposto di se stesso.

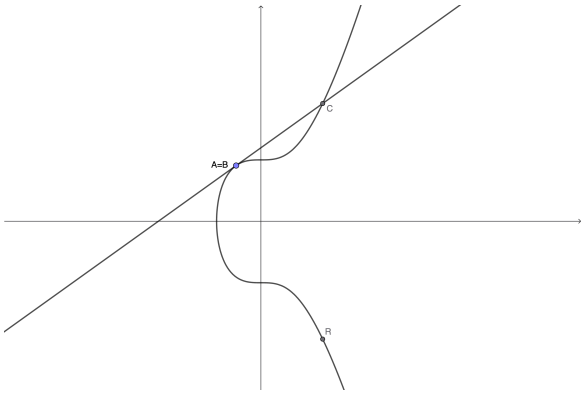


Fig. 3: Curva non singolare $y^2 = x^3 + 7$ definita su $\mathbb{R}$

Proposizione 1 *$(E, +)$ è un gruppo abeliano con elemento neutro $\mathcal{O}$.*

Osservazione 1 *Si noti che in crittografia si considera sempre K campo finito: $\mathbb{Z}_p$ o $\mathbb{F}_q$ con $q = p^n$ e p primo.*

Definizione 4 *Preso k un numero naturale e P un punto di una curva ellittica E, si definisce il prodotto di P per lo scalare k in maniera naturale:*

$$kP = \underbrace{P + P + P + \cdots + P}_{k}$$

cioè la somma di P fatta k volte.
Per definizione se $k = 0$ allora $0 \cdot P = \mathcal{O}$ per ogni P sulla curva.
Se k è negativo si considera il valore assoluto di k e si moltiplica per l'opposto di P: $kP = \mid k \mid [-P]$.

Definizione 5 *Dato un punto P di una curva ellittica E si definisce ordine del punto, se esiste, il più piccolo $m \neq 0$ positivo tale che $mP = \mathcal{O}$.*
Se tale m non esiste si dice che P ha ordine infinito.

Osservazione 2 *Curve ellittiche definite su campi finiti non ammettono punti di ordine infinito.*

Segue la definizione del problema del logaritmo discreto (DLP) per curve ellittiche.

Definizione 6 (ECDLP) *Considerata una curva ellittica E su un campo K e due punti P e Q su E, con P di ordine n e* $Q \in < P >$*, si vuole trovare lo scalare k tale che* $Q = kP$*.*

È immediato notare che, in questo caso, la funzione one-way utilizzata è la moltiplicazione di un punto di una curva ellittica per uno scalare: è facile dato un punto P e uno scalare k, calcolare il prodotto kP tramite le definizioni date precedentemente, ma non è altrettanto facile ricavare k dati P e Q.

Osservazione 3 *Il punto della curva ellittica si chiama* ***punto base*** *ed è, per definizione, un punto della curva dal quale si calcolano, tramite moltiplicazione per scalari, altri punti della stessa. In crittografia si considerano curve ellittiche di ordine primo così che ogni punto (eccetto l'elemento neutro) sia un generatore; in questo modo si è sicuri che lo spazio delle chiavi sia il più grande possibile. Infatti, per ottenere la chiave privata, scelto il punto base* $P \neq \mathcal{O}$ *e preso uno scalare k,* $1 \leqslant k \leqslant N - 1$ *(dove N è l'ordine di P), si costruisce la chiave pubblica calcolando kP. Poiché per il teorema di Lagrange l'ordine di ogni elemento del gruppo* $(E, +)$ *deve essere un divisore dell'ordine del gruppo* $q = \#E$*, con q primo, allora necessariamente* $N = q$*. Di conseguenza, l'intervallo di scelta per la chiave privata diventa, banalmente,* $1 \leqslant k \leqslant q - 1$*.*

3 Sistema Bitcoin

In ogni applicazione della tecnologia blockchain l'idea di base è principalmente la stessa. All'interno della comunità che decide di utilizzarla, gli utenti possono scambiarsi risorse digitali (crittovalute, documenti, etc). Come detto in precedenza per poter identificare in qualche modo gli utenti essi posseggono uno o più account e una coppia di chiavi, privata e pubblica; la chiave privata costituisce la firma digitale dell'utente mentre quella pubblica identifica l'account stesso. Affinché ci sia scambio di risorse digitali è necessario che il possessore delle stesse stipuli e pubblichi in un registro una transazione in cui specifica uno o più destinatari e il contenuto della condivisione. La transazione proposta deve essere corretta, cioè deve essere firmata dal mittente tramite chiave privata; la correttezza della transazione deve essere espressa, poi, dalla comunità che deve verificare la firma digitale del mittente utilizzando la sua chiave pubblica. Una transazione considerata corretta, viene successivamente raggruppata a transazioni corrette pubblicate da altri utenti in un blocco. Tale blocco, affinché ci sia davvero la cessione/condivisione delle risorse in oggetto, deve essere pubblicato e considerato valido. Chiunque riesca a

risolvere un determinato puzzle, cioè un problema imposto dal sistema, può proporre la pubblicazione del blocco; tale processo è chiamato *"mining"* e quest'ultimo ha diversi modelli a seconda dei casi. La validazione del blocco proposto e dunque delle transazioni che contiene è ottenuta grazie ad un processo molto importante chiamato *"ricerca dei consensi"* che ha anch'esso diversi modelli. Infine per pubblicare un blocco valido è necessario che questo sia collegato ad un blocco già esistente nel registro tramite funzioni hash. La catena di blocchi così formata costituisce la blockchain stessa [11].

3.1 Transazioni Bitcoin

La risorsa digitale oggetto delle transazioni nel sistema BTC è, chiaramente, la moneta bitcoin. Una transazione è costituita dai seguenti campi.

- **Metadata**. Contiene informazioni riguardanti la transazione stessa:
  - data di creazione dei dati;
  - dimensione;
  - numero di identificazione della transazione.
- **Input**. Consiste in:
  - mittente della transazione;
  - numero di identificazione di una o più transazioni precedenti in cui il mittente è stato destinatario;
  - firma digitale del mittente.
- **Output**:
  - indirizzo di uno o più destinatari;
  - la somma di bitcoin da trasferire.

Nel protocollo BTC, il trasferimento di moneta richiede il riferimento esplicito alle transazioni in cui il mittente è stato precedentemente destinatario. In un sistema decentralizzato, privo di autorità centrali di garanzia, tale meccanismo è indispensabile per validare il passaggio di proprietà: il mittente dimostra la legittimità del possesso citando le transazioni la cui moneta intende spendere.

Una transazione Bitcoin è corretta se sono verificate due condizioni:

- la firma digitale del mittente è corretta;
- i bitcoin che si vogliono trasferire non sono stati già spesi.

Prima di essere pronte per essere inserite nei blocchi da produrre tramite mining, le transazioni Bitcoin hanno necessità di essere considerate *valide*. Ogni transazione contiene uno Script, cioè una parte di codice scritto in un linguaggio di programmazione specifico che può essere eseguito automaticamente. Ogni nodo deve eseguire lo Script della transazione per validarla. Il linguaggio utilizzato ha le seguenti caratteristiche:

- è stato costruito appositamente per il sistema BTC;
- è stack-based: ogni istruzione viene eseguita una sola volta quindi non ci sono loop;
- non è completo secondo Turing, cioè non può essere utilizzato per qualsiasi funzione o algoritmo arbitrariamente complesso.

Il linguaggio Script di Bitcoin si compone ad oggi (2019) di 256 istruzioni, di cui 166 risultano attualmente operative, 75 rimangono riservate per utilizzi futuri e 15 sono state disabilitate per ragioni di sicurezza. Il set di istruzioni spazia da operazioni aritmetiche e logiche elementari a primitive crittografiche avanzate, incluse funzioni hash e protocolli per la verifica delle firme digitali.

Il funzionamento di un sistema decentralizzato è garantito dai miner, i quali sono incentivati a includere le transazioni nei blocchi attraverso le commissioni (transaction fees). In ogni transazione, la commissione spettante al miner è calcolata come differenza tra il totale dei bitcoin in input e quelli in output. Sebbene non sia obbligatorio includere una commissione, una ricompensa esigua riduce drasticamente la probabilità che i miner selezionino la transazione, poiché essi tendono a dare priorità a quelle più remunerative per massimizzare il proprio profitto.

3.2 Generazione delle chiavi

La partecipazione alla rete Bitcoin in qualità di nodo richiede una connessione Internet e l'impiego di un wallet per la gestione delle transazioni. Seguendo gli standard della tecnologia blockchain, il portafoglio si avvale di una chiave privata e di una chiave pubblica; quest'ultima, come accennato in precedenza, viene derivata dalla prima mediante il processo di generazione previsto dall'algoritmo crittografico ECDSA.

La curva ellittica usata dal sistema Bitcoin è la cosiddetta $Secp256k1$, secondo la classificazione *Standards for Efficient Cryptography (SEC)* ed è definita dall'equazione

$$y^2 = x^3 + 7 \tag{1}$$

Il sistema BTC utilizza $Secp256k1$ [8] definita sul campo F_p con

$$p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$$

Il punto base è $P = (P_x, P_y)$, dove in rappresentazione esadecimale:

$$P_x = \texttt{79BE667E F9DCBBAC 55A06295 CE870B07}$$
$$\texttt{029BFCDB 2DCE28D9 59F2815B 16F81798}$$

$$P_y = \texttt{483ADA77 26A3C465 5DA4FBFC 0E1108A8}$$
$$\texttt{A6855419 9C47D08F FB10D4B8}$$

Come visto precedentemente la chiave privata deve essere compresa tra 1 e $N-1$ dove N è l'ordine del punto base P:

$$1 \leqslant k \leqslant N-1.$$

Il gruppo abeliano G definito dalla curva ellittica sul campo F_p, sappiamo che è un gruppo finito. Con algoritmi di calcolo si ottiene facilmente che la cardinalità di G è il numero primo:

$$\begin{aligned} q = & 1157920892373161954235709850086879078528375642790749043826051631415181614943 \end{aligned}$$

Dunque G è ciclico e un qualsiasi punto scelto in esso, escluso l'elemento neutro $\mathcal{O}$, avrà ordine pari a q stesso, quindi è un generatore di G. Lo spazio delle chiavi private, allora, è costituito dal campo degli scalari ${\mathbb{Z}_q}^*$.

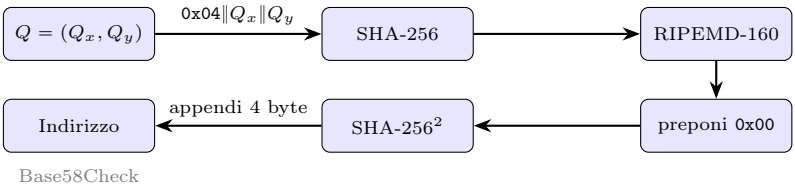
Infine, a partire da una chiave privata $k \in {\mathbb{Z}_q}^*$, si ottiene la chiave pubblica corrispondente semplicemente moltiplicando k per il punto base P:

$$k \cdot P = Q$$

3.3 Generazione degli indirizzi BTC

Ottenuta la chiave pubblica $Q = (Q_x, Q_y)$, l'algoritmo di generazione degli indirizzi Bitcoin prevede l'utilizzo di due funzioni hash, SHA-256 e RIPEMD-160. Dato un input di massimo $2^{64}-1$ bit SHA-256 restituisce, dopo le fasi di "padding", "block decomposition" e diverse operazioni logiche (XOR, AND, OR, etc), un output di 256 bit. RIPEMD-160 ("Race Integrity Primitives Evaluation Message Digest") comprime un input di lunghezza arbitraria in un digest di 160 bit. Una volta applicate le hash function alla chiave pubblica per ottenere l'indirizzo finale bisogna riscrivere il risultato in base 58; questa codifica prevede l'uso delle cifre da 1 a 9, le lettere dell'alfabeto minuscole e maiuscole escluse "O", "I", "l" i cui caratteri sono simili.

Di seguito l'intero algoritmo che genera gli indirizzi Bitcoin.



Algorithm 1: Bitcoin Address Generator

1 **Input:** Chiave privata $k \in \mathbb{Z}_q^*$

2 **Output:** Indirizzo Bitcoin

1. Calcolare la chiave pubblica $Q = kP = (Q_x, Q_y)$ moltiplicando k per il punto base di Secp256k1 tramite ECDSA;
2. costruire la stringa di 65 byte: $\underbrace{\texttt{0x04}}_{\text{1 byte}} \parallel \underbrace{Q_x}_{\text{32 byte}} \parallel \underbrace{Q_y}_{\text{32 byte}}$;
3. applicare SHA-256 seguita da RIPEMD-160 alla stringa del passo 2;
4. preporre il byte `0x00` al risultato del passo 3;
5. applicare SHA-256 due volte al risultato del passo 4;
6. concatenare i primi 4 byte del risultato del passo 5 in coda al risultato del passo 4 (checksum);
7. codificare la stringa in Base58 per ottenere l'indirizzo Bitcoin.

Abbiamo visto precedentemente che la curva ellittica $Secp256k1$ usata nel sistema Bitcoin ha un numero di punti q dell'ordine grande di 2^{255} circa.

Poiché, come spiegato, le chiavi private variano in ${\mathbb{Z}_q}^*$ non si può pensare di applicare un attacco brute force al sistema Bitcoin. Dato quindi un indirizzo Bitcoin o la relativa chiave pubblica, il problema del logaritmo discreto ha complessità esponenziale visto l'ordine del primo q e quindi di $q-1$. Stiamo allora dicendo che è impensabile, poiché computazionalmente impossibile al momento, provare ad invertire la funzione

$$\begin{aligned} \phi : {\mathbb{Z}_q}^* &\longrightarrow G \\ k &\longrightarrow k \cdot P \end{aligned}$$

Si è pensato allora di provare un attacco brute force su un sottogruppo H del gruppo ${\mathbb{Z}_q}^*$, con un numero di elementi non troppo grande. Prese le chiavi in H se si calcolano tutte le chiavi pubbliche corrispondenti è come invertire la restrizione

$$\phi_H : H \longrightarrow G.$$

Per questo il primo obiettivo è stato generare un sottogruppo del gruppo moltiplicativo ${\mathbb{Z}_q}^*$ di chiavi private e, a partire da queste, generare gli indirizzi Bitcoin; il secondo verificare l'eventuale presenza di questi nella blockchain del sistema Bitcoin.

In particolare, dati $p_1 = 107361793816595537$, $p_2 = 174723607534414371449$ e $p_3 = 3419484869741660005223436092831 89$, la fattorizzazione di $q-1$ è:

$$q - 1 = 2^6 \cdot 3 \cdot 149 \cdot 631 \cdot p_1 \cdot p_2 \cdot p_3.$$

– Preso un elemento primitivo di $\mathbb{Z}_q^*$ (in particolare $t = 7$) e posto $w = p_1 \cdot p_2 \cdot p_3$, abbiamo costruito il sottogruppo $H = \langle g \rangle$ generato da $g = t^w$, di ordine $2^6 \cdot 3 \cdot 149 \cdot 631 = 18051648$:

$$H = \langle g \rangle = \left\{ g^i \mid i \in [1, 18051648] \right\}.$$

– Abbiamo generato gli indirizzi Bitcoin a partire dalle chiavi private in H.
– Abbiamo verificato la presenza di tali indirizzi nella blockchain. Ricordiamo che gli indirizzi presenti nel registro pubblico sono quelli coinvolti in almeno una transazione; la loro presenza attesta l'esistenza di un portafoglio attivo associato.

Osservazione 4 *La scelta dell'elemento primitivo t del campo $\mathbb{Z}_q^*$ è, in linea teorica, arbitraria. Tuttavia, nell'implementazione computazionale tramite il software* Magma *che abbiamo utilizzato, la ricerca degli elementi avviene in ordine sequenziale per ottimizzare l'efficienza del calcolo; di conseguenza, il programma restituisce sistematicamente il minimo elemento generatore. Per tale ragione, nel caso specifico in esame, si è adottato il valore $t = 7$, in quanto risulta essere il primo elemento primitivo individuato dall'algoritmo di ricerca del software.*

La fase iniziale di ricerca ha fornito riscontri significativi: l'indagine ha permesso di individuare quattro indirizzi Bitcoin realmente esistenti, da noi generati, le cui chiavi private sono risultate appartenere al sottogruppo H. È doveroso precisare che due di tali chiavi presentano valori banali, nello specifico 1 e -1. Di seguito si riportano gli indirizzi identificati; si è scelto tuttavia di omettere le relative chiavi private per evidenti ragioni di sicurezza e riservatezza:

1. `1PSRcasBNEwPC2TWUB68wvQZHwXy4yqPQ3`
2. `1B5USZh6fc2hvw2yW9YaVF75sJLcLQ4wCt`
3. `1JPbzbsAx1HyaDQoLMapWGoqf9pD5uha5m`
4. `1EHNa6Q4Jz2uvNExL497mE43ikXhwF6kZm`

Abbiamo proceduto con la verifica empirica della nostra metodologia, fornendo la prova del possesso delle chiavi private associate agli indirizzi individuati.

Al fine di validare i risultati ottenuti, abbiamo inizialmente predisposto un portafoglio Bitcoin opportunamente finanziato. Successivamente, è stata trasferita una frazione di bitcoin verso l'indirizzo `1PSRcasBNEwPC2TWUB68wvQZHwXy4yqPQ3` e, una volta confermata la transazione, abbiamo provveduto alla restituzione dei fondi verso il nostro portafoglio d'origine. Tale operazione è stata resa possibile dall'utilizzo della chiave privata derivata per l'indirizzo target, confermando così l'effettiva vulnerabilità dello stesso.

Nella Tabella 1 sono riportate le specifiche per verificare quanto appena detto.

#	Transaction ID	Descrizione
1	`88060229b8bc638ce007c2 27cd4b7185c2f891c2ed4b 85ffd09e6ab96d5abcae`	Trasferimento di una quota di bitcoin per il finanziamento dell'indirizzo `1FCuka8PYyfMULbZ7fWu5GWVYiU88KAU9W`.
2	`69ad7033376cea2bbea01e 7ef76cc8d7bc028325e917 9b2231ca1076468c1a1e`	Trasferimento di 0,002 BTC verso l'indirizzo vulnerabile `1PSRcasBNEwPC2TWUB68wvQZHwXy4yqPQ3`; i restanti BTC trasferiti verso `1NChjA8s5cwPgjWZjD9uu12A5sNfoRHhbA`, gestito dal nostro wallet.
3	`1dd5c256a1acc81ea4808a 405fd83586ea03d8b58e29 a081ebf3d0d95e77bf63`	Trasferimento dei fondi dall'indirizzo vulnerabile verso `1695755gMv3fJxYVCDitMGaxGu7naSXYmv`, attestando il pieno controllo sulla chiave privata derivata.
4	`b722c77dcdd13c3616bf0c 4437f2eb63d96346f74f4e eb7a1e24c1a9711fc101`	Ritrasferimento di tutti i BTC all'indirizzo iniziale `1FCuka8PYyfMULbZ7fWu5GWVYiU88KAU9W`.

Table 1: Transazioni Bitcoin a conferma della vulnerabilità.

Osservazione: Abbiamo scelto di fornire la prova del possesso della chiave privata associata all'indirizzo 1PSRcasBNEwPC2TWUB68wvQZHwXy4yqPQ3 sulla base di precise valutazioni qualitative. Escludendo gli indirizzi con chiavi banali, tale target presentava le caratteristiche tipiche di un portafoglio ad uso personale, a differenza dei cosiddetti *puzzle addresses*, spesso generati intenzionalmente come esche per i cracker. L'analisi dello storico ha infatti rivelato che l'indirizzo ha mantenuto un saldo costante, equivalente a circa 270 dollari, per un periodo di quattro anni, fino al 12 febbraio 2018.

4 Attacchi simili in letteratura

Il contributo presentato raccoglie una riesposizione divulgativa di risultati già pubblicati in [7], qui riproposti per renderli accessibili a un pubblico più ampio. L'attacco descritto si inserisce in una famiglia ben nota di vulnerabilità legate alla scarsa qualità dell'entropia nella generazione delle chiavi; vale quindi la pena richiamare brevemente i più significativi in letteratura.

Nonce non casuali in ECDSA. La sicurezza di ECDSA dipende in modo critico dall'utilizzo di un nonce k nuovo e uniformemente casuale per ogni firma. Qualora k venga riutilizzato anche una sola volta, la chiave privata è immediatamente recuperabile per sottrazione algebrica. Due episodi reali hanno coinvolto questo principio. Nel 2010, la console PlayStation 3 di Sony firmava tutti i messaggi con lo stesso valore di k, consentendo a fail0verflow di estrarre la chiave privata master e pubblicare la firma del firmware arbitrario [3]. Nel 2013, un difetto nel generatore `SecureRandom` di Java su Android causava la produzione di nonce con entropia insufficiente; numerosi wallet Bitcoin ne furono colpiti e fondi per svariate centinaia di migliaia di dollari risultarono vulnerabili o sottratti [1].

Generatori pseudocasuali difettosi nella generazione delle chiavi. Un'ulteriore classe di attacchi riguarda la debolezza strutturale dei generatori pseudocasuali (PRNG) impiegati nella produzione delle chiavi private. Heninger *et al.* [4] hanno dimostrato che un numero significativo di chiavi RSA e DSA pubblicamente disponibili condivideva fattori primi, imputabile a PRNG con entropia iniziale insufficiente su dispositivi embedded. Analogamente, Lenstra *et al.* [5] hanno analizzato un ampio corpus di certificati X.509 giungendo a conclusioni simili. In tutti questi casi, la struttura matematica del problema resta la riduzione dello spazio effettivo delle chiavi, che rende praticabile una ricerca esaustiva.

La congettura del Cryptolab, qui presentata. L'ipotesi alla base dell'attacco descritto in questo articolo fu formulata dal Cryptolab nel 2017 [2] e applicata sperimentalmente l'anno successivo. L'osservazione di partenza è di natura puramente algebrica: se un wallet genera una chiave iniziale $g \in H \leqslant \mathbb{Z}_q^*$ e produce le chiavi successive come potenze iterate $g, g^2, g^3, \ldots$, allora tutte appartengono necessariamente al medesimo sottogruppo H. Ne consegue che la sicurezza effettiva del portafoglio non è quella dell'intero spazio $\mathbb{Z}_q^*$, bensì quella del solo sottogruppo H, il cui ordine può essere di molti ordini di grandezza inferiore. Il caso esaminato in questo articolo, con $|H| \approx 1{,}8 \times 10^7$, ne è una dimostrazione empirica diretta.

5 Conclusioni

Sebbene il nostro approccio [7] abbia individuato solo un numero esiguo di indirizzi generati da chiavi private appartenenti al sottogruppo considerato, è fondamentale sottolineare come tale risultato risulti comunque inaspettato. Al momento della nostra analisi (Giugno 2018), si contavano circa

$$M = 4,5 \cdot 10^8$$

indirizzi Bitcoin apparsi sulla blockchain. La nostra indagine si è focalizzata su un campione di

$$N = 18.051.648$$

indirizzi, ovvero quelli derivanti dalle chiavi private contenute nel sottogruppo H.

Il numero massimo di indirizzi distinti possibili è pari a

$$R = 2^{160},$$

che si presumono tutti esistenti, data la distribuzione uniforme di SHA-256 e RIPEMD-160. Pertanto, la probabilità teorica di individuare almeno un indirizzo esistente sulla blockchain effettuando N campionamenti casuali era pari a:

$$1 - \prod_{i=0}^{N-1} \left(1 - \frac{N}{R-i}\right) \simeq 5,6 \cdot 10^{-33}.$$

Si evince chiaramente che, se le chiavi private Bitcoin fossero state generate in modo puramente casuale, la probabilità di riscontrare anche un solo indirizzo sarebbe stata pressoché nulla.

Le ragioni dietro il verificarsi di un evento così statisticamente improbabile possono essere molteplici. È verosimile che ciò dipenda dagli algoritmi di generazione pseudo-casuale (o dalle loro specifiche implementazioni) adottati dai wallet per creare gli indirizzi degli utenti. La congettura, formulata dal Cryptolab nel 2017, e applicata l'anno successivo, trae origine da un principio fondamentale della teoria dei gruppi: se $g \in H \leqslant G$, allora $g^a \in H$ per ogni intero a. Di conseguenza, qualora le chiavi private vengano derivate tramite potenze iterate, è sufficiente che il wallet generi una singola chiave all'interno di un determinato sottogruppo affinché tutte le chiavi successive appartengano inevitabilmente al medesimo insieme. Tale dinamica produce una drastica riduzione dello spazio di ricerca effettivo, confinando la sicurezza del portafoglio entro un perimetro significativamente più ristretto e vulnerabile rispetto alle previsioni teoriche.

Ringraziamenti: Ringrazio il prof. Massimiliano Sala per avermi dato la possibilità di frequentare uno stage presso l'Università degli Studi di Trento e per avermi fatto da supervisore al progetto di ricerca; ringrazio il prof. Roberto La Scala, dell'Università degli studi di Bari per l'opportunità di collaborazione fornita e per aver fatto da supervisore alla mia tesi di laurea. Ringrazio il dott. Daniele Taufer per la fondamentale collaborazione per la buona riuscita del progetto stesso.

References

1. Android Developers Blog. Security fix for android's java cryptography architecture, 2013.
2. Cryptolab, Università degli Studi di Trento. Congettura sulla struttura dei sottogruppi nello spazio delle chiavi Bitcoin, 2017. Comunicazione interna, citata in [7].
3. fail0verflow. Console hacking 2010: PS3 epic fail, 2010. 27th Chaos Communication Congress (27C3).
4. Nadia Heninger, Zakir Durumeric, Eric Wustrow, and J. Alex Halderman. Mining your Ps and Qs: Detection of widespread weak keys in network devices. In *Proceedings of the 21st USENIX Security Symposium*, pages 205–220, 2012.
5. Arjen K. Lenstra, James P. Hughes, Maxime Augier, Joppe W. Bos, Thorsten Kleinjung, and Christophe Wachter. Ron was wrong, Whit is right. In *IACR ePrint Archive*, 2012. Report 2012/064.
6. Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008. Self-published.
7. Massimiliano Sala, Domenica Sogiorno, and Daniele Taufer. A small subgroup attack on bitcoin address generation. *Mathematics*, 2020.
8. Standards for Efficient Cryptography Group. Recommended elliptic curve domain parameters: `secp256k1`, 2010.
9. Douglas R. Stinson. *Cryptography: Theory and Practice*. Chapman & Hall/CRC – Taylor & Francis Group, 3 edition, 2006.
10. Lawrence C. Washington. *Elliptic Curves: Number Theory and Cryptography*. Chapman & Hall/CRC – Taylor & Francis Group, 2 edition, 2008.
11. Dylan Yaga, Peter Mell, Nik Roby, and Karen Scarfone. Blockchain technology overview. Technical Report NIST IR 8202, National Institute of Standards and Technology, January 2018.

Part III
Applicazioni

Le stablecoin nella rivoluzione silenziosa del denaro: tra geopolitica e finanza.

Vincenzo Vespri*

Università di Firenze, Dipartimento di Matematica ed Informatica "Ulisse Dini"
Viale Morgagni 67/a, 50134 Firenze
vincenzo.vespri@unifi.it

Abstract. Il denaro sta cambiando pelle, e lo fa in silenzio nel codice invisibile delle blockchain. Le *stablecoin*, criptovalute legate al valore di valute tradizionali, sono diventate protagoniste di una rivoluzione poco compresa, ma percepita a livello globale.
Questa nota intende offrire un'introduzione divulgativa a questo oggetto controverso, analizzando la sua origine storica, il contesto di instabilità delle criptovalute originali come Bitcoin, e il suo ruolo come ponte tra la finanza tradizionale e quella decentralizzata. Verranno inoltre esplorati i tentativi di creare stablecoin di Stato e le loro implicazioni geopolitiche, dal fallimentare Petro venezuelano alla corsa globale alle CBDC.

1 Introduzione

La digitalizzazione dell'economia sta trasformando profondamente il modo in cui il valore viene creato, trasferito e conservato. In questo processo, le criptovalute hanno introdotto nuovi modelli di organizzazione monetaria fondati su reti decentralizzate e tecnologie blockchain [32], aprendo un dibattito che coinvolge non soltanto aspetti tecnologici e finanziari, ma anche questioni di natura istituzionale e geopolitica.

All'interno di questo scenario, le stablecoin rappresentano una delle innovazioni più rilevanti emerse nell'ultimo decennio. Si tratta di strumenti digitali progettati per mantenere un valore relativamente stabile attraverso il collegamento a valute tradizionali, materie prime o altre attività finanziarie [9]. Nate come risposta alla forte volatilità delle prime criptovalute, esse hanno progressivamente assunto un ruolo centrale nell'ecosistema blockchain, favorendo l'integrazione tra finanza tradizionale e finanza decentralizzata.

De Cifris Koine – BITCOIN & BLOCKCHAIN
https://doi.org/10.69091/koine/vol-6-B07

* Membro Gnampa (Istituto Nazionale dell'Alta Matematica). Il lavoro è stato parzialmente finanziato dal progetto PRIN deTOKoDe (DEsigning a governance for the TOKenised ecOnomy in a Decentralised Era).

La loro diffusione ha rapidamente superato i confini delle comunità tecnologiche che ne avevano promosso lo sviluppo iniziale. Oggi le stablecoin vengono impiegano nei mercati delle criptovalute, nelle applicazioni della finanza decentralizzata, nei pagamenti internazionali e nei trasferimenti di valore su scala globale. Parallelamente, la loro crescita ha attirato l'attenzione di governi, banche centrali e autorità di vigilanza, che vedono in tali strumenti una potenziale fonte di innovazione, ma anche una possibile sfida alla stabilità finanziaria e al tradizionale monopolio statale dell'emissione monetaria.

Il dibattito contemporaneo sulle stablecoin va quindi ben oltre la loro dimensione tecnica. Esso investe temi quali la sovranità monetaria, il ruolo delle banche centrali nell'era digitale, la regolamentazione delle infrastrutture finanziarie globali e la crescente influenza esercitata da soggetti privati nella gestione dei sistemi di pagamento. In questo senso, le stablecoin si collocano al crocevia tra innovazione tecnologica, politica economica e competizione geopolitica.

L'obiettivo di questo contributo è fornire una panoramica introduttiva del fenomeno delle stablecoin, analizzandone l'origine, l'evoluzione e le principali implicazioni economiche e istituzionali. Dopo aver illustrato le caratteristiche fondamentali di questi strumenti, verranno richiamati alcuni precedenti storici che mostrano come forme di moneta privata abbiano accompagnato lo sviluppo dei sistemi economici in diverse epoche. Sarà quindi esaminata l'evoluzione delle criptovalute e il problema della volatilità che ha favorito la nascita delle stablecoin. L'analisi si concentrerà successivamente sui principali modelli oggi esistenti, sulle diverse strategie di regolamentazione adottate a livello internazionale e sul rapporto tra stablecoin, valute digitali di banca centrale e nuove forme di sovranità monetaria. Particolare attenzione sarà dedicata alle esperienze degli Stati Uniti e dell'Unione Europea, che rappresentano due approcci differenti alla gestione dell'innovazione finanziaria digitale.

Prima di procedere, è opportuno chiarire alcuni termini che nel dibattito pubblico vengono spesso utilizzati in modo intercambiabile. Con il termine criptovaluta si indica l'insieme delle attività digitali basate su tecnologie crittografiche e blockchain, tra cui rientrano Bitcoin, Ethereum e numerosi altri token. Le stablecoin costituiscono una particolare sottocategoria di criptovalute progettata per mantenere un valore relativamente stabile mediante il collegamento a valute ufficiali, attività finanziarie o altri meccanismi di stabilizzazione. Con l'espressione moneta digitale si farà invece riferimento, in senso più generale, a qualsiasi forma di denaro rappresentata in formato elettronico, indipendentemente dalla tecnologia utilizzata o dal soggetto emittente. Infine, le Central Bank Digital Currencies (CBDC) rappresentano una specifica forma di moneta digitale emessa direttamente da una banca centrale e costituiscono quindi la versione digitale della moneta pubblica.

L'ipotesi interpretativa che guida questo lavoro è che le stablecoin non costituiscono semplicemente una nuova categoria di attività finanziarie digitali. Esse rappresentano una manifestazione concreta della più ampia trasformazione che sta

interessando il sistema monetario contemporaneo, caratterizzata da una ridefinizione dei rapporti tra tecnologia, finanza e potere politico. Comprendere il loro sviluppo significa quindi osservare una delle dinamiche più significative attraverso cui si sta ridisegnando l'architettura monetaria del XXI secolo.

2 Ma cosa sono le stablecoin e come funzionano?

Le stablecoin sono una particolare categoria di criptovalute progettata per mantenere un valore relativamente stabile nel tempo [9]. A differenza di Bitcoin, Ethereum e di molte altre criptovalute, il cui preço è determinato esclusivamente dalle dinamiche di mercato, le stablecoin mirano a ridurre la volatilità attraverso un collegamento con attività considerate più stabili, generalmente valute tradizionali come il dollaro statunitense o l'euro.

Il principio di funzionamento è relativamente semplice. Nel caso più diffuso, ogni unità di stablecoin emessa corrisponde a una quantità equivalente di attività detenute in riserva dall'emittente [11]. Se, ad esempio, una società emette un miliardo di token ancorati al dollaro, essa dovrebbe detenere attività di valore equivalente, costituite da liquidità, depositi bancari o strumenti finanziari a basso rischio. In queste condizioni, il possessore della stablecoin può teoricamente convertirla in qualsiasi momento nella valuta di riferimento secondo un rapporto di cambio prefissato.

L'obiettivo fondamentale di questo meccanismo è combinare la stabilità delle valute tradizionali con le caratteristiche operative della tecnologia blockchain. Le stablecoin consentono infatti di trasferire valore in modo rapido, programmabile e potenzialmente globale, mantenendo al tempo stesso un'esposizione limitata alle oscillazioni di prezzo tipiche delle criptovalute tradizionali.

Questa caratteristica ha favorito una rapida diffusione delle stablecoin all'interno dell'ecosistema digitale. Esse svolgono oggi un ruolo centrale nei mercati delle criptovalute, dove vengono utilizzate come strumento di regolamento delle transazioni e come forma di conservazione temporanea della liquidità. Parallelamente, le stablecoin costituiscono una delle infrastrutture fondamentali della finanza decentralizzata (*decentralized finance*, DeFi) [10, 11], permettendo l'accesso a servizi di prestito, investimento e scambio senza il ricorso agli intermediari finanziari tradizionali.

L'utilizzo delle stablecoin si è progressivamente esteso anche oltre il settore delle criptovalute. In alcuni contesti esse vengono impiegate nei pagamenti internazionali, nelle rimesse transfrontaliere e nella gestione della tesoreria aziendale. In Paesi caratterizzati da elevata inflazione o da sistemi bancari fragili, le stablecoin denominate in dollari rappresentano inoltre uno strumento alternativo per preservare il valore dei risparmi e facilitare l'accesso a una valuta considerata più stabile.

La crescente diffusione di questi strumenti è riconducibile principalmente alla loro capacità di ridurre uno dei principali limiti delle criptovalute originarie: la volatilità [9, 32]. Se Bitcoin è stato concepito come un sistema monetario decentralizzato indipendente dalle autorità centrali, la forte instabilità del suo valore ne ha limitato

l'utilizzo come mezzo di pagamento e unità di conto. Le stablecoin cercano di superare questa difficoltà, offrendo una forma di moneta digitale caratterizzata da una maggiore prevedibilità del valore.

Tuttavia, la stabilità promessa dalle stablecoin dipende dalla solidità dei meccanismi che ne garantiscono il funzionamento. La fiducia degli utenti è strettamente legata alla qualità delle riserve, alla trasparenza degli emittenti e alla possibilità di verificare che le attività dichiarate siano effettivamente disponibili. Alcuni episodi verificatisi negli ultimi anni hanno mostrato come carenze nei controlli, nella governance o nella gestione delle riserve possano compromettere la credibilità di tali strumenti [2, 8, 20].

La diffusione delle stablecoin solleva inoltre interrogativi di natura economica e regolamentare. Se quote crescenti di pagamenti e risparmi vengono gestite attraverso strumenti emessi da soggetti privati, quali saranno le conseguenze per il sistema bancario tradicional? Quale ruolo potranno continuare a svolgere le banche centrali nella gestione della politica monetaria [5, 4]? E in che modo le autorità pubbliche dovranno intervenire per garantire stabilità, trasparenza e tutela degli utenti?

Le stablecoin rappresentano quindi molto più di una semplice innovazione tecnologica. Esse costituiscono un tentativo di conciliare la flessibilità delle infrastrutture blockchain con la stabilità richiesta da qualsiasi sistema monetario destinato a essere utilizzato su larga scala. Per questa ragione occupano oggi una posizione centrale nel dibattito sul futuro del denaro digitale e sull'evoluzione dei rapporti tra finanza, tecnologia e sovranità monetaria.

3 Le radici storiche delle stablecoin

Le stablecoin vengono spesso presentate come una delle innovazioni più originali emerse dall'ecosistema delle criptovalute. In realtà, l'idea di strumenti monetari emessi da soggetti diversi dallo Stato ha accompagnato gran parte della storia economica. Sebbene le tecnologie utilizzate siano radicalmente diverse, molte delle questioni sollevate oggi dalle stablecoin — dalla credibilità dell'emittente alla qualità delle riserve, fino al rapporto con le autorità pubbliche — trovano significativi precedenti storici.

La storia monetaria mostra infatti che la produzione e la circolazione del denaro non sono sempre state monopolio degli Stati. In numerose epoche, soprattutto quando le istituzioni pubbliche si sono dimostrate incapaci di garantire strumenti di pagamento adeguati alle esigenze dell'economia, soggetti privati o comunità locali hanno sviluppato forme monetarie alternative.

Un primo esempio significativo è rappresentato dalla Firenze tra il XIII e il XV secolo. In quel periodo la città costituiva uno dei principali centri finanziari europei e le grandi famiglie bancarie, tra cui i Bardi, i Peruzzi e i Medici, svolgevano un ruolo fondamentale nei traffici commerciali internazionali. Il fiorino d'oro, introdotto nel 1252, divenne rapidamente una delle monete più affidabili e diffuse del continente

pur trattandosi di una moneta pubblica emessa dalla Repubblica fiorentina [31]. La sua ampia accettazione non derivava soltanto dall'autorità politica della città, ma soprattutto dalla reputazione commerciale e finanziaria delle istituzioni che ne sostenevano la circolazione. L'esperienza fiorentina mostra come la credibilità economica possa rappresentare un elemento essenziale per il successo di uno strumento monetario.

Situazioni analoghe si verificarono nelle colonie europee del continente americano tra il XVII e il XVIII secolo. La scarsità di oro e argento rese spesso difficile l'utilizzo delle tradizionali monete metalliche, inducendo le comunità locali a sperimentare forme alternative di pagamento. In alcune regioni furono utilizzati beni come il tabacco o lo zucchero, mentre nel Massachusetts comparvero le prime emissioni di cartamoneta delle Americhe [22]. In Canada, durante il periodo dell'amministrazione francese, vennero persino impiegate carte da gioco ufficialmente validate dalle autorità coloniali come mezzo temporaneo di scambio [7]. Sebbene molto diverse tra loro, queste esperienze rispondevano a una medesima esigenza: garantire la considerazione del valore in contesti nei quali gli strumenti monetari tradizionali risultavano insufficienti.

Un precedente ancora più vicino alla logica delle moderne stablecoin può essere individuato negli Stati Uniti del XIX secolo, prima dell'istituzione della Federal Reserve [23]. In quel periodo numerose banche private emettevano proprie banconote convertibili in oro o argento. La loro affidabilità dipendeva dalla capacità dell'istituto emittente di mantenere la promessa di conversione e dalla qualità delle riserve detenute. Alcune emissioni godevano di un'ampia accettazione, mentre altre risultavano caratterizzate da elevata incertezza. Il sistema era frammentato e spesso inefficiente, ma evidenziava un principio destinato a riemergere nel dibattito contemporaneo: il valore di uno strumento monetario dipende in larga misura dalla credibilità dell'emittente e dalla fiducia che esso riesce a generare presso gli utilizzatori.

Nel corso del Novecento il sistema monetario internazionale si orientò progressivamente verso forme sempre più centralizzate. Gli accordi di Bretton Woods del 1944 crearono un ordine monetario fondato sul dollaro statunitense convertibile in oro e sulle principali valute nazionali collegate al dollaro [26]. La fine della convertibilità decretata dagli Stati Uniti nel 1971 segnò il passaggio definitivo all'era della moneta fiat, il cui valore non deriva da una riserva materiale, ma dalla credibilità delle istituzioni che la emettono e dalla loro capacità di preservarne il potere d'acquisto [1].

Negli ultimi decenni del XX secolo, l'espansione delle reti informatiche e lo sviluppo della crittografia alimentarono nuove riflessioni sulla possibilità di creare forme di denaro digitale indipendenti dalle autorità centrali. I movimenti dei *cypherpunk* furono tra i primi a elaborare progetti orientati alla costruzione di sistemi monetari decentralizzati, capaci di garantire privacy, autonomia e resistenza alla

censura. Da queste esperienze sarebbero successivamente emersi Bitcoin [32] e, in una fase successiva, le stablecoin.

Oggi il dibattito sulle forme monetarie alternative non riguarda più soltanto comunità tecnologiche o ambienti accademici. Le trasformazioni dell'economia digitale e le tensioni geopolitiche internazionali hanno riportato al centro dell'attenzione il tema della sovranità monetaria. Iniziative promosse da gruppi di Paesi come i BRICS, così come i progetti di valute digitali sviluppati da numerose banche centrali, testimoniano la ricerca di nuove infrastrutture finanziarie capaci di ridurre la dipendenza dai sistemi tradizionali dominati dal dollaro [5, 4].

Osservati in questa prospettiva storica, le stablecoin appaiono meno come una rottura radicale e più come l'ultima manifestazione di una tendenza ricorrente. In diverse epoche, infatti, l'evoluzione economica e tecnologica ha favorito la nascita di strumenti monetari sviluppati al di fuori dei canali tradizionali. Ciò che distingue le stablecoin dai loro predecessori non è tanto la funzione economica svolta, quanto il contesto tecnologico globale nel quale operano.

4 La nascita delle criptovalute e il problema della volatilità

Per comprendere l'origine delle stablecoin è necessario esaminare il contesto nel quale esse sono emerse. Le prime criptovalute nacquero infatti con l'ambizione di creare una nuova forma di denaro digitale indipendente dagli Stati e dagli intermediari finanziari tradizionali. Tuttavia, fin dalle loro prime fasi di sviluppo, esse si confrontarono con un problema che ne avrebbe limitato l'utilizzo come mezzo di pagamento: la forte volatilità del valore [3, 9].

La storia delle criptovalute inizia ufficialmente nell'ottobre del 2008, quando un autore identificato con lo pseudonimo di *Satoshi Nakamoto* pubblicò il documento intitolato *Bitcoin: A Peer-to-Peer Electronic Cash System* [32]. In quel lavoro veniva proposto un sistema di pagamento elettronico decentralizzato, fondato su una rete distribuita e sulla registrazione delle transazioni all'interno di un registro pubblico condiviso, successivamente noto come *blockchain*.

La pubblicazione avvenne nel pieno della crisi finanziaria globale, in un periodo caratterizzato da una diffusa sfiducia nei confronti delle istituzioni bancarie e finanziarie. Non sorprende quindi che Bitcoin venisse presentato come un'alternativa ai sistemi monetari tradizionali, capace di operare senza il controllo di governi o banche centrali [1]. Lo stesso *Genesis Block*, il primo blocco della blockchain di Bitcoin, conteneva un riferimento al salvataggio delle banche britanniche durante la crisi, a testimonianza della forte componente ideologica che accompagnò il progetto fin dalle sue origini.

Nei primi anni Bitcoin rimase un fenomeno limitato a una ristretta comunità di sviluppatori e appassionati di crittografia. Progressivamente, tuttavia, la criptovaluta iniziò ad acquisire valore economico e ad attirare l'attenzione di investitori, imprese

e media. La crescita del prezzo fu accompagnata da oscillazioni sempre più ampie, trasformando Bitcoin in un'attività finanziaria altamente speculativa.

Parallelamente, le caratteristiche di pseudonimato offerte dal sistema favorirono il suo utilizzo in mercati digitali non regolamentati. Il caso più noto fu quello di *Silk Road*, una piattaforma online chiusa dalle autorità statunitensi nel 2013, che contribuì ad associare nell'immaginario collettivo le criptovalute ad attività illegali. Sebbene tale rappresentazione fosse parziale e spesso fuorviante, essa contribuì ad accrescere la notorietà di Bitcoin e a intensificare il dibattito pubblico sul ruolo delle nuove tecnologie monetarie.

Negli anni successivi l'ecosistema delle criptovalute conobbe una rapida espansione. Nel 2015 venne lanciato Ethereum, ideato da Vitalik Buterin [10], che introdusse il concetto di *smart contract* e trasformò la blockchain da semplice infrastruttura monetaria a piattaforma programmabile per applicazioni decentralizzate. Questa innovazione aprì la strada a nuovi modelli economici e finanziari, ma non risolse il problema della volatilità. Anche l'Ether, la criptovaluta nativa della rete Ethereum, fu caratterizzato da forti oscillazioni di prezzo.

Tra il 2016 e il 2018 il settore visse una fase di crescita estremamente rapida, alimentata dal fenomeno delle *Initial Coin Offering* (ICO), che consentivano a nuove iniziative imprenditoriali di raccogliere capitale attraverso l'emissione di token digitali [3]. Accanto a progetti innovativi emersero numerosi casi di speculazione e di frode, contribuendo a rafforzare la percezione delle criptovalute come strumenti ad alto rischio. Nello stesso periodo il settore fu interessato da importanti episodi di instabilità. Il fallimento dell'exchange Mt. Gox nel 2014 e altri attacchi informatici mostrarono le vulnerabilità operative delle nuove infrastrutture digitali, mentre le forti oscillazioni dei prezzi alimentarono un ciclo continuo di espansioni e contrazioni del mercato.

Nonostante queste difficoltà, le criptovalute continuarono a diffondersi e ad attrarre l'interesse di investitori istituzionali, imprese tecnologiche e governi. La Cina avviò i primi programmi sperimentali per una valuta digitale di banca centrale, mentre altri Paesi iniziarono a valutare il possibile utilizzo delle tecnologie blockchain in ambito finanziario e monetario [4]. Le criptovalute cessarono così di essere un fenomeno confinato alle comunità tecnologiche, assumendo una crescente rilevanza economica e geopolitica.

Rimaneva tuttavia irrisolto il problema che aveva accompagnato Bitcoin fin dalla sua nascita [3, 9]. Il valore delle principali criptovalute era soggetto a variazioni talvolta estremamente rapide e significative. Una caratteristica compatibile con attività speculative, ma difficilmente conciliabile con le funzioni tradizionalmente attribuite alla moneta, quali mezzo di pagamento, unità di conto e riserva di valore. La volatilità limitava infatti la possibilità di utilizzare le criptovalute nelle transazioni quotidiane e rendeva complessa la pianificazione economica sia per i privati sia per le imprese. L'adozione su larga scala richiedeva strumenti in grado di conservare i vantaggi della tecnologia blockchain — trasferibilità globale, programmabilità e

riduzione degli intermediari — senza rinunciare alla stabilità necessaria per le attività economiche ordinarie.

Fu proprio da questa esigenza che nacque l'idea delle stablecoin [9, 11]. L'obiettivo non era sostituire Bitcoin o le altre criptovalute, bensì affiancarle con strumenti digitali caratterizzati da una minore variabilità del valore. Attraverso il collegamento a valute tradizionali, materie prime o altre attività finanziarie, le stablecoin cercarono di fornire all'ecosistema blockchain una componente monetaria più stabile e prevedibile. In questa prospettiva, le stablecoin possono essere interpretate come una risposta ai limiti economici emersi durante la prima fase di sviluppo delle criptovalute. Esse rappresentano il tentativo di combinare l'innovazione tecnologica introdotta dalla blockchain con le caratteristiche di stabilità richieste da qualsiasi sistema monetario destinato a un utilizzo diffuso [2, 11].

5 Il Petro: il primo esperimento di stablecoin statale

L'affermazione delle stablecoin ha rapidamente mostrato che tali strumenti non rappresentano soltanto un'innovazione tecnologica, ma possono assumere una rilevanza economica e geopolitica significativa. Se inizialmente esse furono concepite come una risposta alla volatilità delle criptovalute, ben presto emerse la possibilità di utilizzarle anche come strumenti di politica monetaria e di proiezione strategica da parte degli Stati.

In questa prospettiva, il caso del *Petro* occupa una posizione particolare nella storia delle valute digitali [1]. Annunciato nel dicembre 2017 e lanciato ufficialmente nel 2018 dal governo venezuelano guidato da Nicolás Maduro, il Petro rappresentò il primo tentativo di creare una stablecoin emessa direttamente da uno Stato sovrano [21]. Per completezza, sebbene il Petro venga generalmente classificato come il primo tentativo di stablecoin statale, la reale esistenza e verificabilità delle garanzie sottostanti è stata ampiamente contestata.

Il progetto venne presentato come una criptovaluta garantita dalle ingenti riserve petrolifere del Paese e destinata a fornire una nuova infrastruttura monetaria capace di sostenere l'economia nazionale. L'iniziativa nacque in un contesto estremamente difficile. Negli anni precedenti il Venezuela era stato colpito da una grave crisi economica caratterizzata da iperinflazione, contrazione della produzione e progressiva perdita di valore della moneta nazionale. Secondo le stime del Fondo Monetario Internazionale, nel 2018 l'inflazione superò il milione per cento annuo [27]. Parallelamente, le sanzioni economiche imposte dagli Stati Uniti e da altri Paesi occidentali limitavano l'accesso del governo ai mercati finanziari internazionali e rendevano più complessa la raccolta di capitali dall'estero.

In questo scenario il governo venezuelano individuò nelle tecnologie blockchain una possibile soluzione. Il Petro avrebbe dovuto essere un token digitale ancorato alle riserve petrolifere nazionali e utilizzabile nei pagamenti internazionali senza dipendere dai circuiti finanziari tradizionali [21]. Nelle intenzioni dei promotori, esso

avrebbe consentito al Paese di attrarre investimenti, recuperare credibilità finanziaria e ridurre gli effetti dell'isolamento economico.

Fin dalle prime fasi, tuttavia, il progetto incontrò ostacoli significativi [13]. Il principale riguardava la credibilità dell'emittente e la verificabilità delle garanzie dichiarate. Gli investitori non disponevano di strumenti indipendenti per accertare l'effettiva consistenza delle riserve petrolifere utilizzate come collaterale né era chiaro il meccanismo attraverso il quale tali risorse avrebbero sostenuto il valore della criptovaluta. A queste incertezze si aggiunsero frequenti modifiche relative all'architettura tecnica del progetto, che alimentarono ulteriori dubbi sulla sua effettiva maturità operativa.

Le difficoltà non furono soltanto di natura tecnica ed economica. L'opposizione venezuelana contestò la legittimità dell'iniziativa, sostenendo che l'utilizzo delle risorse petrolifere nazionali richiedesse l'approvazione dell'Assemblea Nazionale. Sul piano internazionale, nel marzo 2018 gli Stati Uniti vietarono ai propri cittadini e alle proprie imprese qualsiasi transazione collegata al Petro, interpretandolo come un tentativo di aggirare il regime sanzionatorio esistente [13].

Nonostante tali ostacoli, il governo cercò di promuovere l'utilizzo della nuova valuta attraverso misure amministrative e incentivi economici. Alcuni servizi pubblici vennero collegati al Petro e, in diversi momenti, furono annunciati pagamenti di bonus e compensi pubblici denominati nella nuova criptovaluta. Tuttavia, queste iniziative non riuscirono a generare una domanda significativa. La popolazione continuò a preferire il dollaro statunitense o, in misura crescente, stablecoin private come Tether, considerate più affidabili, liquide e facilmente convertibili [38].

Nel corso degli anni il Petro perse progressivamente rilevanza economica. I volumi di scambio rimasero limitati, l'interesse internazionale fu modesto e le infrastrutture dedicate al progetto non raggiunsero mai un livello di utilizzo significativo. Di fatto, il Petro non riuscì a svolgere né il ruolo di moneta nazionale alternativa né quello di strumento efficace per attrarre capitali esteri. La conclusione dell'esperimento arrivò nel 2024, quando le autorità venezuelane decisero di interrompere definitivamente le operazioni associate al Petro e di dismettere le infrastrutture digitali che ne supportavano il funzionamento. Con questa decisione si chiuse il primo tentativo di realizzare una stablecoin emessa da uno Stato sovrano.

Al di là del suo insuccesso operativo, il Petro conserva un'importante rilevanza storica. Esso rappresenta infatti il primo esperimento concreto di utilizzo delle tecnologie blockchain come strumento di politica monetaria nazionale e anticipa molti dei temi che caratterizzano il dibattito contemporaneo sulle valute digitali. L'esperienza venezuelana ha mostrato che la disponibilità di una tecnologia innovativa o di attività utilizzate come garanzia non è sufficiente a garantire il successo di una moneta digitale. La trasparenza delle riserve, la credibilità delle istituzioni emittenti, la stabilità del quadro normativo e la fiducia degli utilizzatori rimangono elementi essenziali [20, 23].

Sotto questo profilo, il caso del Petro costituisce un passaggio importante nell'evoluzione delle monete digitali. Pur essendo terminato con un fallimento, esso ha anticipato molte delle questioni che oggi emergono nella discussione sulle stablecoin regolamentate e sulle valute digitali delle banche centrali. La sua vicenda mostra come la tecnologia possa modificare gli strumenti della politica monetaria, ma non possa sostituire i presupposti economici e istituzionali sui quali ogni sistema monetario continua a fondarsi.

6 Monete digitali e geopolitica: la risposta degli Stati

Il fallimento del Petro non segnò la fine dell'interesse degli Stati per le tecnologie monetarie digitali. Al contrario, l'experience venezuelana contribuì a evidenziare una possibilità destinata a influenzare profondamente il dibattito internazionale: l'utilizzo delle infrastrutture digitali come strumenti di politica monetaria, di innovazione finanziaria e, più in generale, di competizione geopolitica [1, 5].

Negli anni successivi numerosi governi e banche centrali avviarono programmi di ricerca e sperimentazione dedicati alle valute digitali. Le motivazioni erano differenti [4]. Alcuni Paesi cercavano di ridurre la dipendenza dai circuiti finanziari dominati dal dollaro statunitense; altri puntavano a modernizzare i sistemi di pagamento nazionali o a rafforzare il controllo sui flussi monetari interni. In tutti i casi emergeva una medesima consapevolezza: la trasformazione digitale del denaro avrebbe avuto conseguenze rilevanti sugli equilibri economici e politici internazionali [5].

Tra i Paesi maggiormente interessati a queste innovazioni vi è stato l'Iran. Sottoposta da anni a sanzioni economiche e a restrizioni nell'accesso ai principali circuiti finanziari occidentali, la Repubblica Islamica ha mostrato un crescente interesse verso le criptovalute e le tecnologie blockchain. Il Paese è divenuto uno dei principali centri mondiali per il mining di Bitcoin, favorito dalla disponibilità di energia a basso costo, mentre le autorità hanno esplorato diverse soluzioni per facilitare i pagamenti internazionali e mantenere aperti i canali commerciali [30].

Particolare attenzione ha suscitato il progetto discusso con la Russia a partire dal 2023 per la creazione di una valuta digitale garantita dall'oro, destinata agli scambi internazionali [35]. L'iniziativa prevedeva una stablecoin collateralizzata da riserve auree, utilizzabile nei rapporti commerciali tra Paesi interessati a ridurre la dipendenza dal dollaro e dalle infrastrutture finanziarie occidentali. Sebbene il progetto non abbia ancora raggiunto una piena operatività, esso testimonia la crescente ricerca di strumenti monetari alternativi da parte degli Stati soggetti a vincoli geopolitici.

La Russia ha seguito una strategia differente. Dopo l'invasione dell'Ucraina e il conseguente irrigidimento delle sanzioni internazionali, Mosca ha accelerato lo sviluppo del *rublo digitale*, una valuta digitale di banca centrale (*Central Bank Digital Currency*, CBDC) emessa e controllata direttamente dalla Banca Centrale

della Federazione Russa [12]. I programmi pilota avviati nel 2023 sono stati progressivamente ampliati e il progetto è destinato a una diffusione graduale negli anni successivi.

A differenza delle criptovalute tradizionali, il rublo digitale non è stato concepito per garantire decentralizzazione o anonimato. Esso rappresenta piuttosto uno strumento attraverso il quale l'autorità monetaria può aumentare l'efficienza dei pagamenti, migliorare la tracciabilità delle transazioni e rafforzare l'integrazione tra sistema monetario e politiche economiche nazionali. Parallelamente, il progetto si inserisce nella più ampia strategia russa volta a sviluppare infrastrutture finanziarie meno dipendenti dai circuiti controllati dalle economie occidentali.

Il caso più avanzato rimane tuttavia quello della Cina. Diversamente dal Venezuela, Pechino non ha puntato su stablecoin private né su soluzioni ibride, ma ha scelto di sviluppare una vera valuta digitale di banca centrale. Lo *yuan digitale* (*e-CNY*) rappresenta oggi il più esteso programma di sperimentazione di una CBDC a livello mondiale [6, 34]. Milioni di cittadini cinesi hanno già avuto accesso al sistema attraverso programmi pilota e applicazioni integrate nelle principali piattaforme di pagamento del Paese.

Sul piano interno, lo yuan digitale consente di aumentare l'efficienza delle transazioni e offre alle autorità monetarie una visibilità senza precedenti sui flussi finanziari. Sul piano internazionale, esso costituisce uno strumento attraverso il quale la Cina può promuovere l'utilizzo della propria valuta negli scambi commerciali e rafforzare la propria autonomia rispetto alle infrastrutture finanziarie dominate dal dollaro.

Accanto a queste strategie orientate al rafforzamento della sovranità monetaria, si colloca il caso particolare di El Salvador. Nel 2021 il governo guidato da Nayib Bukele ha adottato Bitcoin come moneta legale accanto al dollaro statunitense [28]. Pur non trattandosi né di una stablecoin né di una valuta digitale emessa dalla banca centrale, l'iniziativa rappresenta un ulteriore esempio di come le tecnologie monetarie digitali possano essere utilizzate come strumenti di politica economica e di proiezione internazionale. L'obiettivo dichiarato era favorire l'inclusione finanziaria, attrarre investimenti esteri e trasformare il Paese in un centro di innovazione tecnologica. In questo contesto si inseriscono progetti simbolici come la proposta della cosiddetta *Bitcoin City*, concepita come un polo dedicato allo sviluppo dell'economia digitale [24].

Le esperienze di Venezuela, Iran, Russia, Cina ed El Salvador mostrano come le tecnologie monetarie digitali possano essere impiegate per finalità molto diverse. In alcuni casi esse vengono utilizzate per aggirare vincoli economici e sanzioni internazionali; in altri per rafforzare il controllo dello Stato sui sistemi di pagamento; in altri ancora per attrarre investimenti e promuovere nuove strategie di sviluppo economico.

Al di l'à delle differenze, tutte queste iniziative condividono un elemento comune: la consapevolezza che la trasformazione digitale del denaro non rappresenta soltanto

una questione tecnologica. La competizione tra valute tradizionali, stablecoin private e valute digitali di banca centrale è destinata a influenzare gli equilibri economici e geopolitici del XXI secolo [6, 5]. Le nuove infrastrutture monetarie stanno infatti diventando uno dei principali terreni sui quali si confrontano interessi economici, strategie nazionali e modelli alternativi di governance finanziaria. In questo contesto, il dibattito sulle valute digitali non riguarda soltanto il futuro dei sistemi di pagamento, ma anche la ridefinizione dei rapporti di forza all'interno dell'economia globale. La crescente attenzione verso le CBDC e verso le nuove forme di moneta digitale testimonia come la questione monetaria sia tornata a occupare una posizione centrale nelle strategie degli Stati [4, 18, 17].

7 Libra e la sfida delle Big Tech alla sovranità monetaria

Nel giugno del 2019 Facebook annunciò il progetto *Libra*, una delle iniziative più ambiziose mai concepite nel settore delle valute digitali [29]. A differenza di Bitcoin, caratterizzato da una forte volatilità, Libra venne progettata come una stablecoin il cui valore sarebbe stato sostenuto da un paniere di attività finanziarie comprendente le principali valute internazionali, tra cui dollaro statunitense, euro, yen e sterlina. L'obiettivo dichiarato era quello di realizzare un sistema di pagamento globale, stabile e accessibile anche alle popolazioni prive di un adeguato accesso ai servizi bancari [1, 29].

Al di là delle finalità ufficialmente dichiarate, il progetto presentava una portata senza precedenti. Per la prima volta non era uno Stato, una banca centrale o un'istituzione finanziaria internazionale a proporre una nuova forma di moneta destinata a una diffusione globale, bensì una multinazionale tecnologica con oltre due miliardi di utenti distribuiti in quasi tutti i Paesi del mondo. La sola possibilità che una parte significativa di tali utenti potesse adottare Libra come strumento di pagamento fu sufficiente a suscitare l'attenzione delle autorità monetarie internazionali.

La reazione di governi e banche centrali fu immediata [20]. Le autorità compresero rapidamente che Libra non rappresentava soltanto un'innovazione tecnologica, ma una potenziale trasformazione degli equilibri monetari globali. La preoccupazione principale riguardava la possibilità che una piattaforma privata acquisisse un ruolo tradizionalmente riservato agli Stati: l'emissione e la gestione di uno strumento monetario utilizzato su scala internazionale [1, 20].

La peculiarità del progetto risiedeva nella sua struttura. Mentre la maggior parte delle stablecoin esistenti era ancorata a una singola valuta nazionale, Libra avrebbe dovuto essere sostenuta da un paniere di attività finanziarie internazionali. Nelle intenzioni dei promotori, questa scelta avrebbe consentito di ridurre la dipendenza da una singola economia nazionale e di offrire una maggiore stabilità nel lungo periodo. Di fatto, il progetto ambiva a creare una forma di moneta digitale sovranazionale gestita da un soggetto privato [29].

La governance del sistema sarebbe stata affidata alla *Libra Association*, un consorzio internazionale con sede in Svizzera composto da imprese tecnologiche, società di pagamento e altri soggetti privati. Sebbene formalmente il progetto fosse presentato come indipendente da Facebook, la maggior parte degli osservatori riteneva che il gruppo di Menlo Park ne costituisse il principale promotore e beneficiario.

L'importanza di Libra va però oltre la sua struttura tecnica. Il progetto rese evidente una trasformazione più profonda legata all'evoluzione delle grandi piattaforme digitali. Nel corso degli anni, le principali Big Tech hanno costruito ecosistemi che amministrano comunità di utenti paragonabili, per dimensioni, alla popolazione di molti Stati. Esse controllano infrastrutture essenziali per la comunicazione, il commercio elettronico e la gestione dei dati, esercitando una crescente influenza sulle attività economiche e sociali. L'introduzione di una valuta propria avrebbe rappresentato un ulteriore passo verso la costruzione di vere e proprie sovranità digitali private [5].

Le preoccupazioni delle autorità riguardavano diversi aspetti. In primo luogo, vi era il rischio che una diffusione significativa di Libra potesse ridurre la capacità delle banche centrali di influenzare l'economia attraverso gli strumenti tradizionali della politica monetaria [4, 20]. In secondo luogo, permanevano dubbi sulla gestione delle riserve e sulla capacità del sistema di mantenere la stabilità in presenza di crisi finanziarie o richieste massive di conversione. A ciò si aggiungevano questioni legate alla tutela della concorrenza, alla protezione dei dati personali e alla concentrazione di potere economico nelle mani di un numero ristretto di operatori privati.

La dimensione geopolitica era altrettanto rilevante [1, 5]. Una moneta globale controllata da un consorzio dominato da imprese statunitensi avrebbe potuto esercitare un'influenza comparabile a quella delle principali valute internazionali, senza essere soggetta ai meccanismi di controllo democratico che caratterizzano le istituzioni monetarie pubbliche.

Di fronte a queste resistenze, il progetto venne progressivamente ridimensionato. Nel 2020 Libra fu riorganizzata sotto il nuovo nome di *Diem* [14]. La versione originaria, basata su un paniere di valute, venne abbandonata a favore di stablecoin ancorate a singole valute nazionali. Tuttavia, nemmeno questa revisione riuscì a superare le obiezioni delle autorità di vigilanza. Nel gennaio 2022 la Diem Association annunciò la vendita delle proprie attività tecnologiche a Silvergate Capital e l'avvio della liquidazione del progetto, ponendo fine al tentativo di realizzare una stablecoin globale promossa da Facebook [15].

Sotto il profilo operativo, Libra può quindi essere considerata un fallimento. Sotto il profilo storico, tuttavia, il suo impatto è stato notevole. Il progetto dimostrò che una grande piattaforma tecnologica possedeva ormai le capacità finanziarie, organizzative e tecnologiche necessarie per aspirare alla creazione di una moneta globale. Allo stesso tempo, mostrò con chiarezza i limiti politici e regolamentari che tali iniziative avrebbero inevitabilmente incontrato.

L'effetto più significativo di Libra fu probabilmente quello di accelerare il dibattito internazionale sulle valute digitali [4, 17]. Numerose banche centrali intensificarono i propri programmi di ricerca sulle *Central Bank Digital Currencies* (CBDC), mentre i regolatori avviarono la definizione di nuovi quadri normativi dedicati alle stablecoin e ai servizi finanziari basati su blockchain. In Europa, questo processo avrebbe successivamente condotto all'approvazione del regolamento MiCA [19], mentre in altre giurisdizioni si svilupparono iniziative analoghe.

Il principale insegnamento lasciato da Libra è che, nell'economia digitale, la questione monetaria non riguarda più esclusivamente gli Stati e le istituzioni finanziarie tradizionali. Le grandi piattaforme tecnologiche possiedono ormai dimensioni, risorse e capacità operative tali da poter aspirare a un ruolo diretto nella gestione dei sistemi di pagamento e, potenzialmente, della moneta stessa. Sebbene il progetto non sia mai entrato in funzione, esso contribuì a ridefinire il dibattito sul futuro del denaro e rese evidente che la competizione monetaria del XXI secolo avrebbe coinvolto non soltanto governi e banche centrali, ma anche i grandi attori dell'economia digitale.

8 L'evoluzione dei modelli di stablecoin

Le stablecoin nacquero come risposta a uno dei principali limiti delle prime criptovalute: l'elevata volatilità del valore [9, 11]. Se Bitcoin ed Ethereum dimostrarono la possibilità di creare sistemi monetari decentralizzati basati sulla tecnologia blockchain, le forti oscillazioni dei prezzi ne limitarono l'utilizzo come strumenti di pagamento e come unità di conto. Da questa esigenza emerse l'idea di sviluppare monete digitali capaci di mantenere un valore relativamente stabile pur conservando i vantaggi offerti dalle infrastrutture blockchain.

Nel corso degli anni si sono affermati tre principali modelli di stablecoin, differenziati in base al meccanismo utilizzato per garantire la stabilità del valore [2, 9]. Il primo modello è quello delle stablecoin *fiat-collateralizzate*, sostenute da riserve denominate in valute tradizionali [9, 11]. Il secondo è rappresentato dalle stablecoin *crypto-collateralizzate*, garantite da riserve in criptovalute. Il terzo comprende le stablecoin *algoritmiche*, che cercano di mantenere la stabilità attraverso meccanismi automatici di regolazione della domanda e dell'offerta.

La prima categoria è quella che ha conosciuto la maggiore diffusione. In questo modello ogni token emesso dovrebbe essere sostenuto da attività finanziarie di valore equivalente detenute dall'emittente. Il caso più noto è quello di *Tether (USDT)*, lanciato nel 2014 e considerato la prima stablecoin di successo su larga scala [38]. Il progetto si basava su un principio semplice: ogni token doveva corrispondere a un dollaro detenuto nelle riserve della società emittente [2, 23].

Il successo di Tether fu rapido e significativo. Per la prima volta gli operatori del mercato delle criptovalute disponevano di uno strumento che consentiva di trasferire valore in forma digitale senza essere esposti alle continue oscillazioni di Bitcoin. Tuttavia, proprio la centralità del sistema di riserve evidenziò uno dei principali punti

critici del modello. La stabilità del token dipende infatti dalla capacità degli utenti di confidare nell'effettiva esistenza e qualità delle attività detenute dall'emittente. Nel corso degli anni la composizione delle riserve di Tether è stata oggetto di numerose discussioni e verifiche da parte delle autorità di vigilanza e degli operatori di mercato [38].

L'affermazione di Tether favorì la nascita di progetti alternativi caratterizzati da una maggiore enfasi sulla trasparenza e sulla conformità normativa. Tra questi, *USD Coin (USDC)*, sviluppato da Circle e Coinbase nel 2018, si è affermato come uno dei principali concorrenti grazie a procedure di verifica periodica delle riserve e a un rapporto più stretto con il sistema finanziario regolamentato [2].

Accanto alle stablecoin garantite da valute tradizionali emerse un secondo modello, sviluppato con l'obiettivo di ridurre la dipendenza dagli intermediari finanziari. In questa categoria rientra *DAI*, introdotto dal protocollo MakerDAO nel 2017 [11]. Invece di essere sostenuto da depositi bancari, DAI è garantito da riserve in criptovalute bloccate all'interno di smart contract. Per compensare la volatilità del collaterale, il sistema richiede una significativa sovracollateralizzazione: il valore delle garanzie deve risultare superiore a quello dei token emessi [11].

Questo modello presenta il vantaggio di operare in modo più coerente con i principi della finanza decentralizzata, riducendo la dipendenza da soggetti centralizzati [2, 11]. Tuttavia, esso comporta anche costi significativi in termini di efficienza del capitale e rimane esposto ai rischi associati a forti ribassi del mercato delle criptovalute. Nel tempo, inoltre, lo stesso protocollo DAI ha progressivamente integrato nelle proprie riserve anche stablecoin centralizzate, assumendo una struttura più ibrida rispetto alle intenzioni originarie.

Il terzo modello è rappresentato dalle stablecoin algoritmiche. In questo caso la stabilità non viene garantita da riserve esterne, ma da meccanismi automatici progettati per regolare l'offerta monetaria in funzione delle condizioni di mercato. L'esempio più noto è quello di *TerraUSD (UST)*, sviluppato all'interno dell'ecosistema Terra e collegato alla criptovaluta LUNA [8]. Per alcuni anni il progetto venne considerato una delle innovazioni più promettenti dell'intero settore.

Tuttavia, nel maggio 2022, il sistema entrò in una spirale di instabilità che provocò la perdita del rapporto di parità con il dollaro e il successivo collasso dell'intero ecosistema [8]. In pochi giorni vennero distrutti decine di miliardi di dollari di valore di mercato, generando una delle più gravi crisi nella storia delle criptovalute [8, 20]. L'episodio ebbe conseguenze rilevanti sull'intero settore. Da un lato evidenziò la fragilità dei modelli privi di adeguate garanzie patrimoniali; dall'altro rafforzò l'interesse dei regolatori verso sistemi caratterizzati da requisiti più rigorosi in materia di riserve e trasparenza. Il fallimento di TerraUSD contribuì inoltre a influenzare l'evoluzione dei successivi quadri normativi dedicati agli stablecoin [19].

Osservata in prospettiva storica, l'evoluzione delle stablecoin riflette il tentativo di conciliare tre obiettivi spesso difficili da raggiungere simultaneamente: stabilità del valore, decentralizzazione e autonomia dagli intermediari tradizionali [9, 11].

I modelli fiat-collateralizzati privilegiano la stabilità al prezzo di una maggiore centralizzazione; quelli crypto-collateralizzati rafforzano la decentralizzazione ma richiedono un utilizzo meno efficiente del capitale; quelli algoritmici perseguono la massima autonomia dalle riserve esterne, ma hanno mostrato una significativa vulnerabilità nelle fasi di stress del mercato.

Oggi le stablecoin costituiscono una componente essenziale dell'ecosistema blockchain [6]. Esse vengono utilizzate nei mercati delle criptovalute, nella finanza decentralizzata, nei pagamenti internazionali e in numerose applicazioni digitali emergenti. La loro evoluzione mostra come la ricerca di una moneta digitale stabile sia diventata uno degli elementi centrali della trasformazione monetaria in corso. Più che una semplice categoria di strumenti finanziari, le stablecoin rappresentano un laboratorio nel quale vengono sperimentate differenti soluzioni al problema della stabilità monetaria nell'era digitale. La competizione tra i diversi modelli continua ancora oggi e costituisce uno dei principali fattori che influenzeranno l'evoluzione futura dell'intero ecosistema delle valute digitali [6, 5].

9 Le CBDC: la risposta delle banche centrali alle stablecoin

La crescente diffusione delle stablecoin ha posto le banche centrali di fronte a una sfida inedita. Per la prima volta dalla nascita della moneta elettronica, soggetti privati hanno iniziato a offrire strumenti digitali capaci di svolgere alcune delle funzioni tradizionalmente associate al denaro ufficiale. In questo contesto è maturato l'interesse verso le *Central Bank Digital Currencies* (CBDC), ossia valute digitali emesse direttamente dalle banche centrali [4].

L'idea alla base delle CBDC è relativamente semplice [1, 4]. Oggi il denaro esiste principalmente in due forme. Da una parte vi sono le banconote e le monete emesse dalla banca centrale; dall'altra il denaro depositato presso le banche commerciali, che rappresenta un credito nei confronti dell'istituto presso il quale è detenuto. Le CBDC introducono una terza possibilità: detenere e trasferire denaro digitale che costituisce direttamente una passività della banca centrale, senza la necessità di intermediari privati.

Da questo punto di vista, una CBDC può essere interpretata come l'equivalente digitale della banconota. Essa mantiene la natura di moneta pubblica, ma acquisisce le caratteristiche operative tipiche dei sistemi digitali: trasferibilità immediata, programmabilità e integrazione con le moderne infrastrutture di pagamento [4].

Lo sviluppo delle CBDC è strettamente collegato alla diffusione delle criptovalute e, in particolare, delle stablecoin [1, 9]. Se Bitcoin ha mostrato la possibilità di creare sistemi monetari decentralizzati e le stablecoin hanno dimostrato l'esistenza di una domanda crescente di strumenti digitali stabili, le banche centrali hanno iniziato a interrogarsi sull'opportunità di offrire una propria alternativa pubblica. Le CBDC possono quindi essere interpretate come la risposta istituzionale alla trasformazione digitale del denaro [5, 4].

Nonostante alcune somiglianze funzionali, CBDC e stablecoin presentano differenze sostanziali [4, 9]. Le stablecoin sono strumenti emessi da soggetti privati e la loro stabilità dipende dall'esistenza di riserve o da meccanismi di stabilizzazione. Una CBDC, al contrario, non necessita di attività poste a garanzia, poiché rappresenta direttamente la moneta emessa dall'autorità monetaria. La sua validità deriva dal quadro giuridico e istituzionale che sostiene la valuta nazionale.

La possibile introduzione delle CBDC potrebbe modificare in modo significativo il rapporto tra cittadini, banche e Stato [4]. In linea teorica, gli utenti potrebbero detenere una parte del proprio denaro direttamente presso la banca centrale attraverso portafogli digitali dedicati. Una simile trasformazione ridurrebbe il rischio associato agli intermediari privati e aprirebbe nuove prospettive per l'organizzazione dei sistemi di pagamento.

Un aspetto particolarmente innovativo riguarda la programmabilità del denaro [4, 17]. Le CBDC potrebbero consentire l'introduzione di funzioni che non esistono nelle forme monetarie tradizionali, come trasferimenti automatici, pagamenti condizionati o strumenti di sostegno economico destinati a specifiche finalità. Tali possibilità potrebbero rendere più efficaci alcune politiche pubbliche, ma sollevano al tempo stesso interrogativi rilevanti in materia di privacy, controllo delle transazioni e tutela delle libertà individuali.

Le implicazioni delle CBDC non si limitano tuttavia alla dimensione nazionale. Esse possiedono una rilevante componente geopolitica [6, 5]. Il predominio internazionale del dollaro statunitense si fonda anche sul controllo delle principali infrastrutture di pagamento globali. L'introduzione di valute digitali sovrane potrebbe modificare almeno in parte tali equilibri, offrendo a diversi Paesi nuove opportunità di autonomia finanziaria. La Cina rappresenta oggi il caso più avanzato in questo settore. Attraverso lo sviluppo dello yuan digitale, Pechino ha avviato il più ampio programma di sperimentazione di una CBDC a livello mondiale [6, 4, 34]. Anche altre banche centrali, tra cui la Banca Centrale Europea, la Federal Reserve e numerose autorità monetarie dei Paesi emergenti, stanno valutando differenti modelli di implementazione.

Ciò non significa necessariamente che CBDC e stablecoin siano destinati a escludersi reciprocamente. È possibile immaginare un ecosistema nel quale strumenti pubblici e privati coesistano, svolgendo funzioni differenti [5]. Le stablecoin potrebbero continuare a operare come infrastrutture flessibili per la finanza decentralizzata e i pagamenti globali, mentre le CBDC garantirebbero il mantenimento di una forma di moneta digitale direttamente riconducibile alle istituzioni pubbliche.

L'interesse crescente verso le CBDC testimonia come la trasformazione digitale del denaro sia ormai entrata in una nuova fase. Se las stablecoin hanno mostrato che è possibile creare strumenti monetari digitali efficienti e largamente utilizzati, le banche centrali stanno ora cercando di ridefinire il proprio ruolo in questo nuovo contesto. Il dibattito non riguarda soltanto l'innovazione tecnologica, ma il futuro

stesso dell'organizzazione monetaria contemporanea e il rapporto tra sovranità pubblica e iniziativa privata nell'economia digitale [6, 5].

10 Il GENIUS Act e la strategia statunitense per gli stablecoin

La crescita del mercato delle stablecoin ha posto le autorità statunitensi di fronte alla necessità di definire un quadro normativo capace di conciliare innovazione finanziaria e tutela degli utenti. Fino alla metà degli anni Venti, il settore era caratterizzato da una notevole eterogeneità di operatori, modelli di business e regimi di vigilanza. Sebbene gli Stati Uniti ospitassero alcuni dei principali emittenti di stablecoin, mancava una disciplina federale organica che ne regolasse in modo uniforme l'emissione e la circolazione [20].

In questo contesto si colloca il *GENIUS Act* (*Guiding and Establishing National Innovation for U.S. Stablecoins Act*), approvato negli Stati Uniti nel 2025 con l'obiettivo di definire un quadro normativo specifico per le stablecoin destinate ai pagamenti [39]. La legge rappresenta uno dei primi tentativi sistematici di integrare tali strumenti all'interno dell'ordinamento finanziario statunitense, fornendo regole chiare sia per gli emittenti sia per gli utenti [25, 39].

Uno degli aspetti centrali del provvedimento riguarda la definizione giuridica delle stablecoin. La normativa distingue gli strumenti destinati ai pagamenti dalle altre categorie di attività digitali, limitando il nuovo regime regolamentare ai token progettati per mantenere un valore stabile e per essere convertibili in dollari statunitensi in modo rapido e prevedibile [39].

La legge introduce inoltre un sistema di autorizzazione riservato a soggetti sottoposti a vigilanza. Possono emettere stablecoin soltanto banche, istituti autorizzati dall'*Office of the Comptroller of the Currency* oppure operatori che rispettino requisiti normativi equivalenti a livello statale [39, 41]. L'obiettivo è favorire lo sviluppo del settore senza rinunciare a standard minimi di solidità finanziaria e di trasparenza.

Particolare attenzione viene dedicata alla gestione delle riserve. Le stablecoin disciplinate dal GENIUS Act devono essere sostenute integralmente da attività liquide e a basso rischio, quali depositi bancari assicurati, liquidità o titoli del Tesoro statunitense a breve termine [25, 39]. Gli emittenti sono tenuti a pubblicare periodicamente informazioni dettagliate sulla composizione delle riserve e a sottoporsi a verifiche indipendenti [39]. In questo modo la stabilità del valore viene collegata non soltanto all'esistenza delle riserve, ma anche alla loro trasparenza e verificabilità.

La normativa attribuisce inoltre alle autorità pubbliche specifici poteri di intervento in presenza di attività fraudolente, violazioni normative o rischi per la stabilità del sistema [41, 39]. Allo stesso tempo, introduce forme di tutela per i possessori di stablecoin, prevedendo una posizione privilegiata nel rimborso delle riserve in caso di insolvenza dell'emittente. Dal punto di vista istituzionale, il GENIUS Act

produce un effetto rilevante: le stablecoin vengono progressivamente assimilate alle infrastrutture finanziarie regolamentate, evitando le incertezze derivanti dalla loro classificazione come titoli finanziari o *commodity* [25]. Ciò contribuisce a favorire una maggiore integrazione tra il settore delle criptovalute e il sistema finanziario tradizionale.

La legge possiede anche una chiara dimensione strategica. Poiché le riserve devono essere investite in larga misura in attività denominate in dollari e in titoli del Tesoro statunitense, la crescita delle stablecoin regolamentate contribuisce indirettamente a rafforzare la domanda di attività finanziarie statunitensi [5, 39]. In questo senso, l'espansione delle stablecoin può essere interpretata come uno strumento ulteriore di diffusione internazionale del dollaro nell'economia digitale.

Non mancano tuttavia le critiche [41]. Alcuni osservatori ritengono che il nuovo quadro normativo favorisca i grandi operatori già presenti sul mercato, aumentando le barriere all'ingresso per nuove iniziative imprenditoriali. Altri evidenziano le implicazioni derivanti dai poteri attribuiti alle autorità di vigilanza, soprattutto con riferimento alla possibilità di intervenire direttamente sulla circolazione dei token. Tali questioni alimentano un dibattito più ampio sul rapporto tra innovazione, controllo pubblico e tutela della privacy nell'economia digitale.

Al di là dei singoli aspetti normativi, il significato del GENIUS Act risiede soprattutto nella scelta strategica che esso esprime. A differenza di altre giurisdizioni che hanno concentrato l'attenzione sulle valute digitali emesse dalle banche centrali [4, 17], gli Stati Uniti sembrano orientati a valorizzare il ruolo delle stablecoin private, purché inserite all'interno di un quadro regolamentare rigoroso [40, 39].

In questa prospettiva, il dollaro digitale del futuro potrebbe non assumere la forma di una CBDC federale, ma quella di una rete di stablecoin private regolamentate e pienamente integrate nel sistema finanziario statunitense. Il GENIUS Act rappresenta quindi un passaggio significativo nell'evoluzione delle politiche monetarie e finanziarie legate alla blockchain. Esso mostra come la competizione internazionale sulle infrastrutture monetarie digitali non riguardi soltanto l'innovazione tecnologica, ma anche la scelta dei modelli istituzionali attraverso i quali essa viene governata [6, 5].

11 MiCA e la strategia europea per le stablecoin

L'Unione Europea ha affrontato il fenomeno delle stablecoin seguendo un approccio significativamente diverso rispetto a quello adottato dagli Stati Uniti. Mentre la strategia statunitense tende a favorire lo sviluppo di stablecoin private all'interno di un quadro regolamentare dedicato, le istituzioni europee hanno scelto di definire preventivamente un insieme organico di regole volto a garantire stabilità finanziaria, tutela degli utenti e coerenza con l'ordinamento monetario esistente [19].

Il principale strumento attraverso il quale questa strategia è stata implementata è il regolamento *Markets in Crypto-Assets Regulation* (MiCA), approvato nel 2023 ed

entrato progressivamente in vigore tra il 2024 e il 2025. Si tratta del primo tentativo su larga scala di costruire una disciplina organica per le attività digitali all'interno di una grande area economica [19].

Per quanto riguarda le stablecoin, MiCA distingue due categorie principali. La prima comprende gli *E-Money Tokens* (EMT), ossia token ancorati a una singola valuta ufficiale, come l'euro. La seconda è costituita dagli *Asset-Referenced Tokens* (ART), il cui valore dipende da un paniere di attività che può includere valute, strumenti finanziari o altre attività patrimoniali. Entrambe le categorie sono sottoposte a specifici requisiti prudenziali, di trasparenza e di vigilanza [19].

Uno degli aspetti più rilevanti del regolamento riguarda la qualità delle riserve e la tutela degli utenti. Gli emittenti sono tenuti a mantenere attività adeguate a copertura dei token emessi, a garantire procedure di rimborso chiare e a sottoporsi a controlli periodici [19]. L'esperienza di crisi come quella di TerraUSD ha rafforzato la convinzione delle autorità europee che la stabilità monetaria non possa essere affidata esclusivamente a meccanismi algoritmici privi di adeguate garanzie patrimoniali [8]. La normativa ha inoltre introdotto un sistema di autorizzazione centralizzato che consente agli operatori conformi di offrire i propri servizi nell'intero mercato europeo [19]. L'obiettivo è favorire la nascita di un ecosistema regolamentato, capace di combinare innovazione tecnologica e protezione degli utenti.

L'impatto di MiCA è già visibile sul mercato. Alcuni emittenti, come Circle con USDC, hanno ottenuto le autorizzazioni necessarie per operare pienamente nell'Unione Europea [16]. Parallelamente sono state lanciate o annunciate diverse stablecoin denominate in euro, progettate per soddisfare i requisiti della nuova normativa. Altri operatori, tra cui Tether con USDT, hanno invece incontrato maggiori difficoltà nell'adattarsi al quadro regolamentare europeo, determinando una riduzione della loro presenza in alcune piattaforme operanti nell'Unione [38].

Accanto alla regolamentazione delle stablecoin private, l'Europa continua a sviluppare il progetto dell'euro digitale promosso dalla Banca Centrale Europea [18, 17]. Sebbene si tratti di un'iniziativa distinta dalle stablecoin, le due strategie sono strettamente collegate [17]. Da un lato MiCA disciplina gli strumenti emessi da soggetti privati; dall'altro l'euro digitale rappresenta la possibile risposta pubblica alla crescente digitalizzazione dei sistemi di pagamento.

Questa impostazione riflette una caratteristica storica dell'approccio europeo all'innovazione finanziaria. Le istituzioni dell'Unione tendono a privilegiare la costruzione di un quadro normativo stabile prima di favorire una diffusione su larga scala delle nuove tecnologie [19]. Tale scelta presenta vantaggi evidenti in termini di tutela dei consumatori e di riduzione dei rischi sistemici, ma può anche rallentare la velocità di adozione rispetto a contesti normativi più flessibili.

La sfida principale riguarda infatti la capacità di trasformare la regolazione in un vantaggio competitivo. La disponibilità di una disciplina giuridica avanzata costituisce una condizione necessaria, ma non sufficiente, per lo sviluppo di un ecosistema digitale competitivo. Perché gli stablecoin denominati in euro possano

acquisire un ruolo significativo sarà necessario favorirne l'utilizzo nei pagamenti, nei mercati finanziari e nelle applicazioni della finanza decentralizzata [6]. Un ulteriore elemento di complessità deriva dalla dimensione internazionale del fenomeno. Le stablecoin operano su reti globali e competono con strumenti prevalentemente denominati in dollari [6, 5]. Di conseguenza, il successo delle iniziative europee dipenderà non soltanto dalla qualità della regolamentazione, ma anche dalla capacità di creare un'infrastruttura sufficientemente liquida e interoperabile da risultare competitiva a livello internazionale.

Le critiche al modello europeo non sono mancate [19]. Alcuni osservatori ritengono che MiCA imponga oneri eccessivi agli operatori, rischiando di favorire i grandi gruppi finanziari a discapito delle imprese innovative. Altri sostengono invece che proprio la certezza normativa rappresenti uno dei principali punti di forza dell'approccio europeo, soprattutto in un settore caratterizzato da frequenti episodi di instabilità e da un elevato livello di rischio operativo.

In prospettiva, il caso europeo mostra come la competizione sulle valute digitali non riguardi soltanto la tecnologia, ma anche i modelli di governance adottati dalle diverse giurisdizioni [5]. Mentre gli Stati Uniti sembrano orientati a valorizzare il ruolo degli emittenti privati regolamentati [39], l'Unione Europea punta a costruire un equilibrio tra innovazione, supervisione pubblica e sviluppo dell'euro digitale. Il successo di questa strategia dipenderà dalla capacità di trasformare il vantaggio regolamentare in un vantaggio economico e tecnologico. In caso contrario, l'Europa rischierebbe di limitarsi a disciplinare un mercato la cui evoluzione continua a essere guidata prevalentemente da attori esterni all'Unione [6].

12 Tether e il ruolo degli emittenti privati nel mercato delle stablecoin

L'affermazione delle stablecoin non ha prodotto soltanto innovazioni tecnologiche e trasformazioni normative. Essa ha favorito anche l'emergere di nuovi centri di potere economico, legati al controllo delle infrastrutture attraverso cui circolano liquidità e valore nell'ecosistema digitale [5]. In questo contesto, il caso di Tether rappresenta uno degli esempi più significativi.

Fondata nel 2014, Tether è oggi l'emittente della stablecoin USDT, il principale strumento di regolamento utilizzato nei mercati delle criptovalute [38]. Nel corso degli anni il token è diventato una componente essenziale dell'infrastruttura finanziaria dell'intero settore, consentendo agli operatori di trasferire liquidità tra piattaforme, effettuare operazioni di trading e accedere ai mercati digitali senza dover ricorrere continuamente ai circuiti bancari tradizionali [6, 38].

Tra le figure centrali nello sviluppo di Tether vi è Gianfranco Devasini [36, 37], imprenditore italiano che ha contribuito in modo determinante alla crescita della società. Pur mantenendo un profilo pubblico particolarmente riservato, Devasini

è divenuto uno dei protagonisti più influenti dell'economia delle criptovalute, contribuendo alla costruzione di una delle infrastrutture finanziarie private più rilevanti dell'intero settore.

Il successo di Tether deriva principalmente dalla funzione economica svolta da USDT. In un mercato caratterizzato da forte volatilità, la disponibilità di uno strumento relativamente stabile ha consentito di facilitare gli scambi e di ridurre i costi operativi per milioni di utenti [2]. Nel tempo, la stablecoin è diventata il principale punto di riferimento per la gestione della liquidità nei mercati delle criptovalute, raggiungendo livelli di diffusione e utilizzo senza precedenti.

La crescita dell'ecosistema Tether ha tuttavia alimentato anche un intenso dibattito. Nel corso degli anni analisti, autorità di vigilanza e operatori di mercato hanno sollevato interrogativi sulla composizione delle riserve utilizzate a garanzia dei token emessi, sulla trasparenza dei processi di verifica e sul ruolo sistemico assunto dall'azienda all'interno del settore [23, 33, 38]. Tali discussioni riflettono una questione più generale: quanto maggiore è la diffusione di una stablecoin, tanto più rilevante diventa la fiducia riposta nell'emittente e nella qualità delle sue riserve [2, 23]. Nonostante queste controversie, Tether ha consolidato la propria posizione di leadership. Il volume delle transazioni effettuate attraverso USDT ha raggiunto dimensioni comparabili a quelle di importanti infrastrutture finanziarie tradizionali, rendendo la società un attore centrale nell'economia digitale globale [6].

Il caso Tether evidenzia un fenomeno che va oltre la singola vicenda imprenditoriale. Nella nuova economia digitale, il controllo delle infrastrutture può generare forme di potere economico comparabili, e talvolta superiori, a quelle derivanti dalla produzione di beni o servizi [5]. Gli operatori che gestiscono reti di pagamento, sistemi di regolamento e piattaforme finanziarie tendono infatti ad assumere una posizione strategica all'interno degli ecosistemi nei quali operano. Da questo punto di vista, la figura di Devasini assume un valore simbolico. La sua esperienza mostra come una parte crescente della ricchezza e dell'influenza economica contemporanea possa derivare dalla gestione delle infrastrutture che consentono il funzionamento dei mercati digitali. Più che il successo di un singolo imprenditore, il caso Tether rappresenta l'emergere di una nuova categoria di attori economici, capaci di esercitare un'influenza significativa attraverso il controllo delle reti finanziarie digitali.

La vicenda assume inoltre un significato particolare nel contesto europeo. Mentre l'Unione Europea ha scelto di affrontare il fenomeno delle stablecoin attraverso una regolamentazione rigorosa e orientata alla stabilità del sistema [19], uno dei principali protagonisti del settore è un imprenditore italiano che ha sviluppato la propria attività prevalentemente al di fuori del quadro normativo europeo. Questo elemento evidenzia una tensione che caratterizza molte delle tecnologie emergenti: la necessità di trovare un equilibrio tra tutela degli utenti, controllo dei rischi e capacità di sostenere l'innovazione [6, 19].

In tale prospettiva, il caso Tether offre uno spunto di riflessione più ampio sul rapporto tra regolazione e competitività. La questione non riguarda soltanto

il successo di una singola impresa, ma la capacità delle diverse aree economiche di partecipare attivamente alla costruzione delle nuove infrastrutture finanziarie globali. Più in generale, la crescita di operatori come Tether suggerisce che il futuro della moneta digitale potrebbe essere influenzato non soltanto dalle decisioni delle banche centrali e dei governi, ma anche dalle strategie di soggetti privati in grado di controllare infrastrutture utilizzate quotidianamente da milioni di persone [6, 5]. In questo senso, il dibattito sugli stablecoin non riguarda soltanto la tecnologia o la regolamentazione, ma anche la distribuzione del potere economico nell'era digitale.

13 Conclusioni

L'analisi svolta nei capitoli precedenti mostra come le stablecoin rappresentino una delle innovazioni più significative emerse dall'ecosistema blockchain. Nate come risposta alla volatilità delle prime criptovalute, esse si sono progressivamente trasformate in strumenti con implicazioni che vanno ben oltre l'ambito tecnologico e finanziario.

La loro diffusione ha evidenziato l'esistenza di una domanda crescente di strumenti monetari digitali caratterizzati da stabilità, rapidità di trasferimento e integrazione con le infrastrutture digitali globali. Allo stesso tempo, ha reso evidente che il tema della moneta digitale non riguarda soltanto l'efficienza dei sistemi di pagamento, ma coinvolge questioni più ampie legate alla sovranità monetaria, alla regolamentazione dei mercati e alla distribuzione del potere economico.

L'evoluzione delle stablecoin ha inoltre mostrato la coesistenza di modelli profondamente differenti. Le stablecoin garantite da riserve tradizionali hanno privilegiato la stabilità e l'integrazione con il sistema finanziario esistente; quelli collateralizzati da criptovalute hanno cercato di preservare una maggiore decentralizzazione; gli esperimenti algoritmici hanno tentato di eliminare la dipendenza dalle riserve esterne, evidenziando tuttavia significative fragilità operative.

Parallelamente, governi e banche centrali hanno iniziato a elaborare strategie differenti per rispondere alla trasformazione digitale del denaro. L'analisi comparata evidenzia come gli Stati Uniti abbiano scelto di valorizzare il ruolo delle stablecoin private attraverso un quadro normativo dedicato, mentre l'Unione Europea ha privilegiato un approccio maggiormente orientato alla regolazione preventiva e allo sviluppo dell'euro digitale. Altri Paesi, come la Cina, hanno invece puntato direttamente sulle valute digitali emesse dalla banca centrale.

In questo contesto, le stablecoin si collocano al centro di una più ampia competizione tra modelli istituzionali differenti. La questione non riguarda soltanto quale tecnologia prevarrà, ma anche quali soggetti saranno chiamati a gestire le future infrastrutture monetarie. Banche centrali, operatori privati, piattaforme tecnologiche e organismi di regolazione sono oggi coinvolti in un processo di ridefinizione degli equilibri che hanno caratterizzato il sistema monetario negli ultimi decenni.

L'esperienza di progetti come Tether, Libra, il Petro e le prime CBDC mostra che il successo di una moneta digitale non dipende esclusivamente dalla qualità della tecnologia impiegata. La credibilità delle istituzioni coinvolte, la trasparenza dei meccanismi di governance, la solidità delle riserve e l'esistenza di un quadro normativo coerente continuano a rappresentare fattori determinanti.

Le stablecoin non costituiscono dunque una semplice innovazione finanziaria. Esse rappresentano uno dei principali laboratori nei quali si stanno sperimentando le forme future della moneta digitale. La loro evoluzione contribuirà a definire il rapporto tra tecnologia, finanza e potere pubblico nel XXI secolo, influenzando non soltanto il funzionamento dei mercati, ma anche l'architettura istituzionale dell'economia globale.

Acknowledgements L'autore desidera ringraziare R. G. Barresi, A. Bracciali e F. Zatti per le numerose e stimolanti discussioni sui temi trattati in questo lavoro.

References

1. Tobias Adrian and Tommaso Mancini-Griffoli. The rise of digital money, 2019. IMF FinTech Notes.
2. Douglas W. Arner, Raphael Auer, and Jon Frost. Stablecoins: Risks, potential and regulation. (905), November 2020.
3. Raphael Auer, Giulio Cornelli, and Jon Frost. Crypto trading and bitcoin prices: Evidence from a new database of retail adoption, 2022. Bank for International Settlements Working Paper No. 1049.
4. Bank for International Settlements. Central bank digital currencies: Foundational principles and core features, 2020. BIS Report No. 1.
5. Bank for International Settlements. Annual economic report 2023: Blueprint for the future monetary system, 2023. Chapter III.
6. Bank for International Settlements. Annual economic report, 2024. Series 2021–2024.
7. Bank of Canada. A history of the canadian dollar, 2010.
8. Antonio Briola, David Vidal-Tomás, Yuanrong Wang, and Tomaso Aste. Anatomy of a stablecoin's failure: The terra-luna case. *Finance Research Letters*, 51:103358, 2023.
9. Dirk Bullmann, Jonas Klemm, and Andrea Pinna. In search for stability in crypto-assets: Are stablecoins the solution?, 2019. ECB Occasional Paper Series, No. 230.
10. Vitalik Buterin. A next-generation smart contract and decentralized application platform, 2014. Ethereum White Paper.
11. Christian Catalini and Alonso de Gortari. On the economic design of stablecoins, 2021. MIT Sloan School Working Paper.
12. Central Bank of the Russian Federation. Digital ruble project, 2023.
13. Usman W. Chohan. Cryptocurrencies as asset-backed instruments: The venezuelan petro, 2018.
14. Diem Association. Diem white paper, 2020.
15. Diem Association. Statement by diem ceo stuart levey on the sale of the diem group's assets to silvergate, 2022. Press Release, January 31, 2022.

16. European Banking Authority. Mica and stablecoins: Implementation and supervision, 2024.
17. European Central Bank. Report on a digital euro, 2020.
18. European Central Bank. Progress on the investigation phase of a digital euro, 2023.
19. European Parliament and Council. Regulation (eu) 2023/1114 on markets in crypto-assets (mica), 2023. Official Journal of the European Union.
20. Financial Stability Board. Regulation, supervision and oversight of global stablecoin arrangements, 2020.
21. Gobierno de la República Bolivariana de Venezuela. Petro white paper, 2018.
22. Dror Goldberg. The massachusetts paper money of 1690. *The Journal of Economic History*, 69(4):1092–1123, 2009.
23. Gary Gorton and Jeffery Zhang. Taming wildcat stablecoins, 2021. Yale School of Management Working Paper.
24. Government of El Salvador. Bitcoin city initiative, 2022.
25. Bill Hagerty, Kirsten Gillibrand, Tim Scott, and Cynthia Lummis. Guiding and establishing national innovation for u.s. stablecoins (genius) act: Section-by-section analysis, 2025. United States Senate.
26. International Monetary Fund. Articles of agreement of the international monetary fund, 1944.
27. International Monetary Fund. World economic outlook 2018, 2018. Inflation projections for Venezuela.
28. International Monetary Fund. El salvador: 2021 article iv consultation – press release; staff report; and statement by the executive director for el salvador, 2022. IMF Country Report No. 2022/020.
29. Libra Association. An introduction to libra, 2019. White Paper.
30. Library of Congress. Regulation of cryptocurrency around the world: Iran, 2021.
31. Stefano Locatelli. *The Florentine Florin: The Politics and Culture of Money in the Middle Ages*. Manchester University Press, Manchester, 2025.
32. Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008.
33. Office of the New York Attorney General. Virtual markets integrity initiative and tether settlement, 2021.
34. People's Bank of China. Progress of research & development of e-cny in china, 2021.
35. Russian News Agency TASS. Russia and iran discuss gold-backed stablecoin for international trade, 2023.
36. Kadhim Shubber and Siddharth Venkataramakrishnan. Tether's path to the spotlight. Financial Times, 2021. Financial Times investigation on Tether, Bitfinex and their executives.
37. Forbes Staff. L'ex chirurgo plastico e l'informatico: chi sono giancarlo devasini e paolo ardoino, i nuovi miliardari italiani delle criptovalute. Forbes Italia, 2024.
38. Tether Holdings Ltd. Consolidated reserves reports. Various Years.
39. United States Congress. Guiding and establishing national innovation for u.s. stablecoins act (genius act), 2025. Public Law 119–27.
40. U.S. Department of the Treasury. Genius act implementation, 2025. Federal Register.
41. U.S. House Committee on Financial Services. Section-by-section: Guiding and establishing national innovation for u.s. stablecoins act, 2025.

Civic blockchain: tokenized economies supporting local communities

Cristina Viano[2], Irene Domenicale[1,2], Sowelu Avanzo[2], and Claudio Schifanella[2]

[1] University of Camerino, International School of Advanced Studies, Piazza Cavour 19F, 62032 Camerino, Italy
[2] University of Turin, Computer Science Department, Corso Svizzera 185, 10149 Torino, Italy

Abstract. Blockchain technologies hold significant untapped potential for civic and community applications, yet most existing tools remain inaccessible to non-expert users and are poorly aligned with the values of collaborative and social economies. This article presents CommonsHood, a no-code blockchain wallet application designed to enable citizens, associations, and local institutions to create and manage customizable token-based economies without requiring technical expertise.

Drawing on an interdisciplinary theoretical framework, we argue that tokenomic design for local communities must move beyond orthodox market logic and account for the full diversity of human motivations and non-market forms of exchange. CommonsHood addresses this challenge through a factory smart contract pattern supporting multiple token types deployed on a consortium blockchain that eliminates technical barriers. The application has been co-designed and tested through participatory research across multiple real-world pilot projects, spanning urban commons management, youth civic participation, sharing economies, and cultural initiatives.

1 Introduction

The introduction of Bitcoin and, more broadly, blockchain technologies has inaugurated what some researchers describe as an “Internet of Value" revolution: for the first time, it became possible to transfer purely digital objects representing value from one user to another without the need for a trusted intermediary such as a bank or payment processor. This technological shift first enabled the development of decentralized digital currencies. Subsequently, with the introduction of the Ethereum blockchain, it became possible to implement so-called smart contracts — self-executing programs that run on a decentralized computing platform and can

De Cifris Koine – BITCOIN & BLOCKCHAIN
https://doi.org/10.69091/koine/vol-6-B08

automatically enforce agreements between parties. Smart contracts have greatly expanded the range of blockchain applications. In addition to currencies, they enable the creation of arbitrarily complex digital tokens representing assets of various kinds: access rights, vouchers, loyalty instruments, collectibles, governance rights, and more. Yet most of these applications have so far remained in the hands of technologists, who design and deploy token systems according to their own vision and business model, leaving communities as passive users rather than active co-creators. This article argues that blockchain technology has significant untapped potential for civic and community applications and that realizing this potential requires tools that are accessible to non-expert users. We present CommonsHood, an application designed to address exactly this challenge, and describe the experimental research we carried out to develop and test it in real-world community contexts.

2 From De-Fi to blockchain for local communities

2.1 Tokens beyond cryptocurrencies

Tokenomics is the study of how tokens are used within blockchain ecosystems, encompassing token issuance methods, consensus mechanisms, and the broader system of economic and game-theoretic incentives [42]. Rooted in cryptoeconomics, itself defined as the design of systems using cryptography to verify past events and economic incentives to shape future behaviors, tokenomics has evolved to incorporate it as a subset [9, 24]. Its foundations lie in neoclassical economics, particularly the dynamics between supply, demand, and utility, though alternative paradigms grounded in broader socio-economic theories remain an open area of inquiry. Tokenized systems can be understood as complex socioeconomic networks structured across three levels: behavior of individuals, institutionally embedded economic policies, and emerging system properties arising from their interaction [52]. Their inherently interdisciplinary character, bridging economics, governance, computer science, and sociology, demands design approaches that go well beyond conventional market logic. This opens the door to contributions from sociological and anthropological traditions: Zelizer's work on monetary circuits [54], for instance, frames economic transactions not as neutral exchanges but as culturally and socially embedded practices, shaped by the relational contexts in which they occur, while Polanyi's systemic perspective historicalizes the very concepts of economy and market, demonstrating how economic life is always constituted by broader political, historical, and cultural forces [36]. Complementing these perspectives, Ostrom's theory of collective action [30] cautions against reducing all participants to rational egoists. Empirical evidence points to the consistent presence of two additional player types: conditional cooperators, who engage and sustain collaboration so long as reciprocity is perceived, and willing punishers, who enforce community norms by sanctioning free-riders and rewarding generous contributors, even at personal

cost. Accounting for this diversity of motivations is essential to designing token-based systems whose incentive structures and governance mechanisms reflect the cooperative complexity of real human communities.

2.2 Blockchain for Local Communities

Research and experiments defined as blockchain for social good or blockchain for social impact [5, 44] identify several families of applications that go beyond the crypto-finance sector and profit-oriented or industrial applications. These initiatives include domains such as humanitarian aid, microfinance for unbanked populations, NFT-enabled issuance of identity and education certificates in contexts where public institutions are fragile, community currencies and purpose-driven token systems that encourage and acknowledge people's positive contribution to a project. In this domain are also experiments related to civic participation [22], commons-based peer production, universal basic income schemes and more radical alternatives to established neoliberal governance models [38], - which also criticize the very notion of blockchain for "social good" as advanced by mainstream social innovation [41]. These initiatives also intersect with tech sovereignty and FLOSS stances. Among these domains, community-level tokenized economies are particularly relevant to our work. We define blockchain for local communities the initiatives designed to foster active engagement of people and their participation in the social and economic dynamics of socio-geographic contexts [19]. These initiatives use digital tokens designed to circulate within a specific local context to support social and economic exchanges based on cooperation and mutual benefit rather than competition or profit, which include: civic participation process [22], citizen self-organisation and commoning [8], social and solidarity economies [15, 26, 29]. The blockchain's potential for secure value transfer, disintermediation, and trust-building is promising for facilitating the circulation of community assets through token-based economies, by enacting the governance rules of that community through smart contracts that allow to program the transactions of various kinds of tokens. More specifically, utility tokens can represent different forms of monetary and non-monetary, material and immaterial values, such as access rights, skills, time, currencies. For example, individuals may receive reward tokens for performing specific activities, which can then be used to access benefits and services. Utility tokens are particularly interesting from a civic or participatory perspective, when they are defined to reflect the assets and interactions of a local community. A community association could issue tokens that represent hours of volunteering, access rights to a shared workshop, or participation units in a collective purchase initiative. A local municipality could issue tokens to reward citizens who contribute to environmental or cultural activities. A network of small retailers could create a shared loyalty currency circulating within a neighborhood. This flexibility is what makes tokenisation a potentially powerful instrument for community economies — provided that the tools to create and manage

tokens are made accessible to non-technical actor. Governance tokens can allow community members to participate in decision-making processes. Smart contracts can automate the distribution of tokenized assets according to community needs and goals, functioning as rewards or incentives for collaborative work. DAOs can provide decentralized governance infrastructure for organizations requiring horizontal coordination mechanisms, such as citizens associations and cooperatives, by allocating roles and responsibilities in the management of shared resources and spaces. Moreover, if different communities used cryptographic tokens based on common standards, this would enable interoperability and inter-community exchange tokens, collaboration, and resource-sharing.

2.3 Related works

Blockchains are experimented with in projects in the field of collaborative, solidarity and community oriented economies and of related citizens participation process. For instance, in the field of digital commons and of commons-based peer production and consumption, we find speculative design research or attempts to radically re-design consensus mechanism and techno-social governance models [32] [27] [21] [39]. In the same vein, there are toolkit platforms that allow the members of a specific community to create what they need for a particular purpose, from tokens to a DAO, from scratch: Kleros[25], Waves[53], Coinsence[13], Celo[10].Other kinds of tools and non customizable, ready-made platforms that implement specific tokenized models designed for a specific community or project. On one side, there are initiatives where purpose driven tokens are used as rewards and incentives to acknowledge and encourage actions that are deemed positive for the local community in social (e.g. volunteering in municipal activities), economic (e.g. choosing local producers and retailers) or environmental terms (e.g. contributing to environmental protection): examples are Cambiatus [35], Colu[14], Empower[20], Plastic Bank[35], Urban Change[46]. These initiatives are often characterized by high turnover, and are mapped by reports on digital social innovation and databases (see, for instance, [40]), and often are not extensively studied by academic scholars.Conversely, both activists' experiments and scientific research are well established in the field of community and complementary currencies [6] [16] and financial inclusion systems including local credit clearing or universal basic income such as Sarafu Network [28], Monedapar [47], ChainCash [12], Ourvillage [34], PeaceCoin [33], and discontinued cases such as Circles UBI [31] and Faircoin [37].

2.4 Research and experimentation gaps

Although some of these projects have been in existence for some years, others face problems related to financial sustainability, scalability, and the cost of developing or maintaining the technical infrastructure. This makes it difficult for many of

these initiatives to go beyond their pilot or start up phase. Specifically, two significant limitations concern the way in which the tokenized logics underpinning these systems are designed and encoded in blockchain-based tools. First, unlike traditional market-driven models, collaborative economies and civic processes rely on non-market exchange, redistribution, and reciprocity to foster collective agency and social cohesion [17, 36]. Consequently, the community's underlying tokenomics architecture must reflect these values by establishing different user roles and facilitating differentiated interactions. Moreover, in terms of the token functions that are needed, local systems generally require two specific token configurations. Asset Representation: tokens reflecting tangible or intangible assets, structured to satisfy the circulation requirements determined by community values and collaborative economy objectives. Non-Monetary Incentives: tokens operating as catalysts for participation, oriented toward acknowledging and encouraging civic engagement through means that extend beyond financial reward [4]. Second, most existing projects, however well designed, are created by developers and then handed to communities as ready-made tools. The community can use the system but cannot easily modify it or create new kinds of token to suit evolving needs. The technical intricacy of blockchain-based infrastructures creates a clear demand for instruments capable of supporting both the launch and sustained stewardship of community-driven systems, bridging technical architecture with participatory engagement and enabling co-design, capacity building, and a gradual transition toward decentralized governance. From a computer science perspective, this perspective draws on Allen and Potts' framing of the Web3 stack as a set of toolkits [1], a perspective rooted in open innovation theory, where toolkits are understood as coordinated design tools that empower users to develop innovations tailored to their own needs and contexts. Rather than positioning technical expertise and community knowledge as separate domains, this framework treats Web3 infrastructures as systems that embed expert knowledge into protocols, interfaces, and modular components, allowing communities to configure and adapt them to their specific goals

3 The CommonsHood Project

3.1 A customizable wallet-app for local communities

The research project presented in this article addresses the gap mentioned above. Namely, we aim to address the lack of tokenomics design methods which are coherent with the principles and logics of collaborative and social practices, and the lack of blockchain-based platforms in which functionalities and the tokens themselves can be customized to community-specific goals and governance models. Our goal is to advance and validate the civic blockchain approach [50], which aims to make the properties of blockchain and tokenization adaptable and accessible to social and collaborative economies and participatory processes in local communities. A

blockchain based wallet application, named CommonsHood, is both the mean and product of this research. It aims to allow anyone, regardless of technical background, to create new types of tokens that represent assets of value and distribute them through a simple web or mobile interface [3]. In what follows, we provide an overview on the specifics, functionalities, and architecture of the CommonsHood application. We then illustrate some of the pilot projects in which it has been codesigned and tested through participatory research methods. These pilots are the empirical ground for the insights and open research challenges discussed in the final paragraphs. The central technical innovation of CommonsHood is its no-code approach to token creation. Whereas creating a cryptographic token normally requires writing and deploying a smart contract, which is a demanding task in terms of specialized programming languages and understanding of blockchain mechanics, CommonsHood allows users to create tokens by filling in a simple form. The application uses a factory smart contract pattern: a set of pre-audited contract templates, each corresponding to a different type of token, that can be instantiated without writing any code. This approach draws a deliberate parallel with the no-code movement in software development more broadly, which uses graphical interfaces to make programming accessible to non-developers. Just as no-code web builders allow anyone to create a website, CommonsHood allows anyone to create a token-based economic instrument.

3.2 Token Types and Functionalities

CommonsHood supports several types of digital assets, each designed to serve different community needs. Coins are fungible tokens that are used to model prepaid cards, cashback initiatives, and complementary currencies. Once an issuer has created a quantity of a new coin, it can be distributed to users and exchanged freely within the community. Coupons are tokens representing discount vouchers, sharing rights, digital twins of physical objects (such as event tickets), or temporary ownership of a shared resource. Unlike coins, coupons are non-divisible and are consumed upon redemption — once returned to the issuer, they cannot be put back into circulation. Non-fungible tokens (NFTs) allow the creation of unique digital assets, each with its own attributes, that cannot be copied or subdivided. These can represent participation certificates, event tickets, or items in a library of shared objects. CommonsHood makes it possible to create both transferable and non-transferable NFTs, the latter being useful for certificates and badges. The following functionalities enable token transactions among different wallets, enabling manual sending or more complex and programmable interactions. The pay/send function enables the direct transfer of tokens between users and/or activities. Exchanges allow users to offer coins or coupons by asking for other tokens in return, enabling a simple, peer-to-peer token economy within the community. Crowdsales are an instrument for collective fundraising and group purchase. An issuer creates a crowdsale that distributes output coupons to contributors who provide a specified input coin. This

mechanism can model group-buying, cooperative investments, or crowdfunding campaigns. CommonsHood supports liquid crowdfunding, allowing participants to adjust their contribution before the campaign closes. Two additional functionalities extend CommonsHood into the domain of collaborative economies. The Library of Things enables the lending and borrowing of physical objects within a community, using NFTs to track items and fungible tokens to represent rental costs and rewards [48]. The Task Box provides a decentralized platform for community service exchange, combining task management with a dual-token economy inspired by time bank models.

3.3 Architecture and Infrastructure

From a technical perspective, CommonsHood is a decentralized application (dApp) with Technology Readiness Level (TRL) 7. It uses a consortium blockchain — a network with a limited set of known nodes maintained by trusted public actors — rather than a public permissionless blockchain like the main Ethereum network. The consortium blockchain is based on the Ethereum Virtual Machine. The adoption of a consortium blockchain is motivated by the need to relieve users, who often possess limited digital skills, from the operational costs inherent to blockchain technology, such as transaction (gas) fees. To this end, work is currently underway to support transaction sponsorship mechanisms.

The digital assets offered by the platform are implemented through smart contracts and a factory creation pattern: When a new token is created, a Token Factory Smart Contract is called to instantiate a new token contract, starting from a Token Template Smart Contract. The smart contracts underpinning the token system are written in the Solidity language and build on the well-tested OpenZeppelin Contracts library, following established security patterns. Tokens conform to widely adopted standards: the ERC-20 standard for fungible tokens (coins and coupons) and ERC-721 for non-fungible assets. Metadata and documents associated with tokens, including icons, images, and manifests, are stored on the InterPlanetary File System (IPFS), a decentralized file storage network that ensures their immutability and availability. A significant challenge in the design CommonsHood was the management of cryptographic wallets. Typically, using a decentralized blockchain application requires users to manage their own private keys — a technically demanding task that is a major barrier to adoption.

CommonsHood addresses this by providing a seamless wallet management service: users authenticate with a standard username and password through an OAuth2-compliant server, and their cryptographic wallet is created and managed transparently by the platform. This means that users can enjoy the benefits of the blockchain without having to understand its underlying cryptographic infrastructure. Certainly, this approach to wallet management introduces an element of centralization, but we believe that this represents the right balance in terms of the use of the platform.

Wallets can be owned by individuals or be associated with organisations, and be managed by individual wallets of the organization's members with different roles. Organization wallets are also geolocated on an integrated map, which helps making the actors and assets of a geographical content visible. The frontend is implemented in React as a web application, which allows users to access CommonsHood from any device. CommonsHood is also integrated with FirstLife, a civic social network based on an interactive map, that enables geolocalised discovery of community initiatives. Users can find nearby activities, link tokens to physical places via QR codes, and make instant payments in proximity.

4 Methodology and Participatory experimentations

4.1 Iterative co-design and testing of the application

The development of the CommonsHood application has followed an iterative, participatory methodology. Our research group followed a participatory approach to research and adopted service design, user-centered design and participatory co-design methods, working with community actors (urban commons, local associations, municipalities, retailers, and civil society organizations) at each stage of the design and testing process.

The methodology is based on an iterative process of co-design, development, testing and evaluation, which is repeated in different socio-geographic context and focusing on diverse tokenized systems in terms of scope, scale and complexity. In the initial phase of the project, the research team designed and developed the core features of the application, producing a general-purpose version of the platform as a starting point. This general version has then been iteratively and incrementally refined through context-based co-design activities which focus on specific use scenarios and functionalities. First, the socio-economic model of a specific community is studied and co-designed with local actors. Then, the token system and application interface are adapted to support that model. Usability testing and evaluation sessions, which involve both technical and non-technical participants, — provide feedback that feeds back into the next development cycle [49]. This iterative process ensures that the technology evolves in response to real community needs, rather than imposing a predefined technical solution.

4.2 Co-design of tokenized economies

As the project progressed, we refined the co-design process in order to offer a thorough method for co-designing tokenized economies for local communities, of which the customizable application is an essential component. This method is aimed to fill the gaps, mentioned in Section 2, concerning the lack of methods and tools for developing tokenized economies that target the needs and social goals of

civic participation and collaborative economies at the local level. The method is grounded on an interdisciplinary framework which brings together economic sociology, monetary theories, socio-economic geography, tokenomics and token engineering. A core assumption of this framework is that money is socially embedded: it is both grounded in social values and norms, and in turns shapes behaviours [23, 54, 43, 45]. Tokens, as a form of digital money, are something that we can design, on one side, based on the values and characteristics of the social systems that are willing to adopt them, and on the other side aiming at structuring new forms of social interactions (for instance, more participatory). Based on a sociological approach to token engineering, the method is made of four phases which guide the designer and developers to identify the overall purposes of a tokenized and to progressively define its socioeconomic system, its tokenized system, and its specific tokenomics to be reflected in the functionalities and cryptographic assets of the CommonsHood app [18].

4.3 Case studies

The CommonsHood application has been designed, adapted, and tested in a range of real-world contexts through several pilot projects, each focusing on different community needs and token use cases. The initial pilot was carried out within the European projects CO3[3] and Co-City[4] in Turin, focusing on collaborative management of urban commons supported by digital technologies. Community associations in the city's Neighborhood Houses co-designed an "economic urban commoning" scenario in which tokens played multiple roles simultaneously: local coins sold as prepaid cards to citizens, coupons redeemable at local retailers and services, purpose-driven tokens distributed to volunteers, and NFTs used as event tickets issued without collecting personal data [7]. The participatory co-design of services and functionalities implemented during the two projects allowed us to identify a set of viable use scenarios related to economic urban commoning, and to develop and validate core functionalities of the app such as the wallet, token creation, payments, and integration with a geolocated map.

The NLAB4CIT[5] project (2022–2023) tested CommonsHood in the city of Collegno to promote youth civic participation. Young volunteers received reward tokens issued by the municipality, which could be exchanged for coupon tokens offered by local businesses and cultural services. Co-design sessions with local stakeholders defined the terms of the exchange, ensuring that economic incentives complemented rather than displaced social motivations, and provided the real life scenario to test the exchange functionality.

[3] https://cordis.europa.eu/project/id/822615
[4] https://uia.urban-initiative.eu/fr/uia-cities/turin
[5] https://nlab4cit.eu/

The C.O.S.O.[6] project (2023–2024) co-designed a Library of Things in the Turin neighborhood of Borgo Campidoglio, in collaboration with local residents and the District administration. Twelve community members participated in four co-design sessions to define the token model and the user interface. The result was a decentralized object-lending system using NFTs to track shared items and fungible tokens to reward positive community actions [49], which resulted in the dedicated "library of things" functionalities.

The Tecnoprofezie project (2022) explored the use of NFTs in a cultural context, connecting the Museum of Science Fiction in Turin with its community through digital artworks and collectibles, with the explicit aim of promoting community-oriented, rather than speculative, uses of non-fungible tokens.

The BLOCCHI[7] project explored the application of CommonsHood to support sustainable tourism in lesser-visited mountain areas, testing dedicated functionalities and discussing them with local authorities of the Piedmont region in Italy. These functionalities allow retailers and local economic actors to create systems of fidelity tools independently, without relying on commercial intermediary platforms.

The CO.R.PU.S.[8] project (part of the EU DUT Partnership program) has extended CommonsHood to support different models of urban circular and sharing economies. In Turin, the focus has been on a sharing economy that connects demand for items with unused local resources. In Aigaleo (Greece), CommonsHood powered a Community Exchange Hub centered on barter and material upcycling, using community tokens as an internal currency and recognition tokens to acknowledge contributions. The two pilots provide the context in which existing functionalities are further refined and integrated, while also experimenting with more complex tokenomics where different types and uses of tokens are integrated, thus reflecting the daily life of participatory practices.

The FOOD REBORN project operates in the domain of policies aimed at reducing, at the same time, food waste and food poverty. Tokens are backed by the quantities of avoided food waste, and represent forms of community currencies and vouchers that strengthen the access of families in need to goods and services

5 Insights from user evaluation

5.1 Evaluation method and results

The user evaluation of the application is an essential component of the design, development and testing cycle described before, and grounds the iterative refinement of the platform. Evaluations address multiple dimensions: the relevance of

[6] https://www.progettocoso.org/
[7] https://blocchi.di.unito.it/
[8] https://corpusproject.eu/

the application and of the related co-design method for community-based civic process and social economies; its capacity to respond to unsatisfied needs and to trigger transformative social innovations; the effectiveness of the method to introduce complex concepts (such as tokenization) to a non expert public; the usability and accessibility of the app UX and UI. Testing and evaluation sections are implemented through a variety of methods, including formative user studies, usability testing sessions, focus groups, questionnaires and interviews given during either public dissemination events or working sessions with participants to the pilots [51, 11, 49]. CommonsHood represents a distinctive position in the landscape of blockchain applications for communities. Unlike ready-made platforms offering a single pre-defined token economy, it is a customizable platform: a flexible infrastructure that allows different communities to design their own token systems, combining different types of tokens and functionalities according to their specific socio-economic model. At the same time, unlike governance-as-a-service frameworks such as Aragon or DAOstack, which offer powerful but technically demanding tools primarily aimed at complex DAO governance, CommonsHood prioritizes accessibility and local embeddedness, operating on a consortium blockchain that shields users from transaction fees and technical complexity. Some challenges remain. In terms of usability, in most cases pilot users observed that the app is relatively straightforward to use, while also pointing out the need for an introduction in the forms of expert-guided sessions or online tutorials. A recurring request on the side of the users is the addition of an in-app chatting systems to facilitate communications.

5.2 Assessing the civic blockchain experiments

Over the years from the very first testing of the application, a broader skepticism about virtual currencies mostly left place to an interest and curiosity towards tokenized economies. However, tokenization and its mechanisms remain a novel concept which requires training and facilitation. Facilitating the design of tokenized socio-economic models for civic purposes requires interdisciplinary expertise spanning computer science, tokenomics, monetary theory, economic sociology, and participatory design. The disintermediation and automatization logics that are typical of Web3 must be carefully designed in order to enable participatory and collaborative interactions, avoiding the risks of an excess of quantification and stiffening of mutable social relationships [22]. Ensuring that economic incentives embedded in token systems complement rather than displace intrinsic social motivations is a delicate balancing act. The regulatory environment for community currencies and digital tokens remains partially undefined in many jurisdictions, while calling into question well established (but in some cases varying access countries) regulations on currencies, taxation, accountancy. Finally, the risk of digital exclusion — particularly for older or less digitally literate community members — must be continuously addressed through participatory design, accessible interfaces, and hybrid online/offline support

structures, such as material cards with a QR code providing access to a wallet. Despite these challenges, the experiments carried out so far have demonstrated a widespread interest for experimenting with tokenized economies, especially as regards domains such as the social economy, where market-based and community-based logics coexist, and of civic participation, where new forms or citizen engagement are emerging which go beyond traditional forms of social organization. The possibility of creating tokens that make the economic, social, and cultural value of a geographic context emerge appears to be a tool worth exploring in contexts where local authorities, new civil society organization, and social enterprises are rethinking their living, production, and service delivery methods.

6 Conclusions and Future Directions

This article has presented CommonsHood, a blockchain-based wallet application designed to make cryptographic tokenisation accessible to non-expert users in local community contexts. By combining a no-code interface with pre-audited smart contract templates, a consortium blockchain infrastructure that eliminates transaction fees, and a participatory co-design methodology, CommonsHood enables citizens, associations, retailers, and local institutions to create and manage a rich ecosystem of interacting digital tokens — coins, coupons, crowdsales, NFTs, and more. CommonsHood contributes to an emerging research and practice agenda around civic technologies that go beyond the digitization of existing services, instead leveraging the affordances of decentralized infrastructures to enable new forms of democratic and economic participation within local communities. Future work includes the development of native mobile apps, extensions to the token types supported (including governance tokens), and a no-code approach to the deployment of decentralized autonomous organizations (DAOs) based on visual modeling. In this respect, we aim to develop a no-code approach by integrating the work concerning the development of a low code approach for the specification and development of DAOs based on visual models, named DAO-ML. This currently includes tool support enabling the generation of smart contracts from visual governance models. This is described in [2]. Further interdisciplinary research will also focus on refining the co-design frameworks and analytical tools used to model tokenized economies for social purposes.

Acknowledgments This research was funded by: Italian Ministry of University and Research under the Driving Urban Transitions Partnership - Call 2022 (project "CORPUS - Phygital Cooperation in the Retrofitting of Public Space). MUR (“Borse di Dottorato” - Dottorato di Ricerca di Interesse Nazionale in “Blockchain and Distributed Ledger Technology”, under the National Recovery and Resilience Plan (NRRP) 963.

The authors declare that they developed the application described in this work and conducted the associated evaluation. No financial or commercial conflicts of interest are associated with this study

References

1. Darcy WE Allen and Jason Potts. Web3 toolkits: A user innovation theory of crypto development. *Journal of Open Innovation: Technology, Market, and Complexity*, 9(2):100050, 2023.
2. Sowelu Avanzo, Marco Ottina, Daniele Pautasso, Irene Domenicale, Alex Norta, and Claudio Schifanella. Dao-ml to solidity: A scalable code generation approach for decentralized autonomous organization development. In *Proceedings of the 2025 International Conference on Information Technology for Social Good*, pages 353–361, 2025.
3. Stefano Balbo, Guido Boella, Pierpaolo Busacchi, Alex Cordero, Luca De Carne, Diego Di Caro, Alberto Guffanti, Michele Mioli, Alessandro Sanino, and Claudio Schifanella. Commonshood: A blockchain-based wallet app for local communities. In *2020 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS)*, pages 139–144. IEEE, 2020.
4. Mark C. Ballandies. To incentivize or not: Impact of blockchain-based cryptoeconomic tokens on human information sharing behavior. *IEEE Access*, 10:74111–74130, 2022.
5. Massimo Bartoletti, Tiziana Cimoli, Livio Pompianu, and Sergio Serusi. Blockchain for social good: a quantitative analysis. In *Proceedings of the 4th EAI international conference on smart objects and technologies for social good*, pages 37–42, 2018.
6. Jérôme Blanc. Classifying 'ccs': Community, complementary and local currencies. *International Journal of Community Currency Research*, 15(D):4–10, 2011.
7. Guido Boella, Claudio Schifanella, and Cristina Viano. Blockchain and tokenisation for local communities. In *Blockchain for Good*, pages 96–116. CRC Press, Boca Raton, FL, 2025.
8. David Bollier and Silke Helfrich. *Free, Fair, and Alive: The Insurgent Power of the Commons*. New Society Publishers, Gabriola Island, BC, 2019.
9. Vitalik Buterin. A next-generation smart contract and decentralized application platform. *white paper*, 3(37):2–1, 2014.
10. Celo. `https://celo.org/`.
11. Samantha Cenere. Locating the alternative digital. care, code, and community for alternative urban economies. *Digital Geography and Society*, 8:100114, 2025.
12. ChainCash. `https://docs.ergoplatform.com/uses/chaincash/`.
13. Coinsence. `https://coinsence.org/`.
14. Colu. Colu local network whitepaper. `https://www.allcryptowhitepapers.com/colu-local-network-whitepaper/`, 2018.
15. Battistoni Como. Economia collaborativa e innovazione nelle imprese cooperative: Opportunità emergenti e sfide per il futuro. *Rivista Impresa Sociale*, 6:97–108, 2015.
16. Eduardo H Diniz, Erica S Siqueira, and Eric Van Heck. Taxonomy of digital community currency platforms. *Information Technology for Development*, 25(1):69–91, 2019.

17. Irene Domenicale, Flavia Fredda, Emanuele Spadaro, and Claudio Schifanella. Participation by design: designing incentives for collaborative economies in local communities. In *7th Distributed Ledger Technologies Workshop (DLT2025)*, 2025.
18. Irene Domenicale, Cristina Toti, and Cristina Viano. Tokenomics design for local communities: Interdisciplinary method for co-design. *Frontiers*, 2026. To appear.
19. Schifanella Domenicale, Viano. Blockchain for local communities: an exploratory review of token economy aspect. *Frontiers in Blockchain*, 7:1426802, 2024.
20. Empower. `https://www.empowerchain.io/`.
21. Fritsch, Emmett, Friedman, Kranjc, Manski, Zargham, and Bauwens. Challenges and approaches to scaling the global commons. *Frontiers in Blockchain*, 4:578721, 2021.
22. Inte Gloerich, Martijn De Waal, Gabriele Ferri, Nazli Cila, and Tara Karpinski. The city as a license. implications of blockchain and distributed ledgers for urban governance. *Frontiers in Sustainable Cities*, 2:534942, 2020.
23. Geoffrey Ingham. The nature of money. *Economic Sociology: European Electronic Newsletter*, 5(2):18–28, 2004.
24. ITO Kensuke. Cryptoeconomics and tokenomics as economics: A survey with opinions. In *2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 729–746. IEEE, 2024.
25. Kleros. `https://kleros.io/`.
26. Gorgi Krlev, Giulio Pasi, Dominika Wruk, and Marika Bernhard. Reconceptualizing the social economy. *Stanford Social Innovation Review*, 2021.
27. S. Manski and M. Bauwens. Reimagining new socio-technical economics through the application of distributed ledger technologies. *Frontiers in Blockchain*, 2, 2020.
28. Carolina E. S. Mattsson, Teodoro Criscione, and William O. Ruddick. Sarafu community inclusion currency 2020–2021. *Scientific Data*, 9:426, 2022.
29. Ethan Miller. Solidarity economy: Key concepts and issues. *Solidarity economy I: Building alternatives for people and planet*, 2010:25–41, 2010.
30. Elinor Ostrom. Collective action and the evolution of social norms. *Journal of economic perspectives*, 14(3):137–158, 2000.
31. Vangelis Papadimitropoulos and Giannis Perperidis. Universal basic income on blockchain: the case of circles ubi. *Frontiers in Blockchain*, 7:1362939, 2024.
32. Kostakis V Pazaitis A, De Filippi P. Blockchain and value systems in the sharing economy: The illustrative case of backfeed. *Technological Forecasting & Social Change*, 125:105–115, 2017.
33. Peacecoin. Whitepaper. `https://peace-coin.gitbook.io/peace-coin/introduction/`, 2025.
34. Jennifer Pédussel Wu, Martina Metzger, Ignacio Silva Neira, and Arafet Farroukh. What determines demand for digital community currencies? ourvillage in cameroon. Technical report, Working Paper, 2023.
35. PlasticBank. `https://plasticbank.com/`.
36. Karl Polanyi. *The Great Transformation: The Political and Economic Origins of Our Time*. Beacon Press, Boston, 1944.
37. Xavier Balaguer Rasillo. Digital commoning and post-capitalist crypto-economies: The case of faircoop. *Geoforum*, 144:103811, 2023.
38. David Rozas, Antonio Tenorio-Fornés, Silvia Díaz-Molina, and Samer Hassan. When ostrom meets blockchain: exploring the potentials of blockchain for commons governance. *Sage Open*, 11(1):21582440211002526, 2021.

39. David Rozas, Antonio Tenorio-Fornés, Silvia Díaz-Molina, and Samer Hassan. When Ostrom meets blockchain: Exploring the potentials of blockchain for commons governance. *Sage Open*, 11:21582440211002526, 2021.
40. Fines SchlumberJ.-A. Blockchains & sustainable development report, association blockchain for good. Available at: https://blockchainforgood.fr/wp-content/uploads/2023/01/Rapport-2022-ok_ENG-V3.pdf., 2022.
41. Silvia Semenzin. 'blockchain for good': Exploring the notion of social good inside the blockchain scene. *Big Data & Society*, 10(2):20539517231205479, 2023.
42. Lisa JY Tan. *Economics and Math of Token Engineering and DeFi: Fundamentals of Token Economics*. Economics Design, english edition edition, November 2020.
43. Bruno Théret. Les trois états de la monnaie. *Revue économique*, 59(4):813–841, 2008.
44. Bill Tomlinson, Jens Boberg, Jocelyn Cranefield, David Johnstone, Markus Luczak-Roesch, Donald J Patterson, and Shreya Kapoor. Analyzing the sustainability of 28 'blockchain for good'projects via affordances and constraints. *Information Technology for Development*, 27(3):439–469, 2021.
45. C. Toti. *La questione della moneta. Riappropriazione del senso di un'istituzione*. TAB Edizioni, Rome, 2024. Monograph, Sezione Scienze Sociali ed Economiche, ISBN: 978-88-9295-822-7.
46. UrbanChange. `https://www.urbanchange.com/`.
47. Sebastian Valdecantos, Ricardo Orzi, Raphaël Porcherot, and Federico José Camargo. Is blockchain a game-changer for social currency systems? some reflections in light of the experience of moneda par in argentina. *Sustainability Science*, 20(4):1195–1209, 2025.
48. Nicolò Vanzo, Emanuele Spadaro, Cristina Viano, and Claudio Schifanella. A blockchain-based object sharing system for local communities. In *Proceedings of the 2024 International Conference on Information Technology for Social Good*, pages 324–332, 2024.
49. Cristina Viano. Context-based civic blockchain: Localising blockchain for local civic participation. *Digital Geography and Society*, 6:100090, 2024.
50. Cristina Viano, Sowelu Avanzo, Guido Boella, Claudio Schifanella, and Vincenzo Giorgino. Civic blockchain: Making blockchains accessible for social collaborative economies. *Journal of Responsible Technology*, 15:100066, 2023.
51. Cristina Viano, Sowelu Avanzo, Monica Cerutti, Alex Cordero, Claudio Schifanella, and Guido Boella. Blockchain tools for socio-economic interactions in local communities. *Policy and Society*, 41(3):373–385, 2022.
52. Shermin Voshmgir, Michael Zargham, et al. Foundations of cryptoeconomic systems. *Research Institute for Cryptoeconomics, Vienna, Working Paper Series/Institute for Cryptoeconomics/Interdisciplinary Research*, 1, 2019.
53. Waves. `https://waves.tech/`.
54. Viviana Zelizer. The social meaning of money. *The American Journal of Sociology*, 95(2):342–377, September 2008.

AI e Blockchain: convergenza tra intelligenza artificiale e fiducia digitale

Davide Carboni

Ingegnere dell'Informazione, Libero professionista

Abstract. Quale potrebbe essere il nesso tra l'intelligenza artificiale e la blockchain? Le due tecnologie, sviluppatesi in modo separato e distinto, rispondono in realtà a bisogni complementari: la **blockchain** fornisce fiducia, tracciabilità e trasparenza; l'**AI** introduce adattività, previsione e automazione. Insieme compongono un paradigma in cui i dati diventano verificabili e le decisioni automatiche sono certificate in modo immutabile.
Questa convergenza si manifesta in varie direzioni: la certificazione dell'origine e integrità dei *dataset* usati per addestrare modelli AI; l'esecuzione di logiche intelligenti in *smart contract* o agenti autonomi *on-chain*; e la creazione di nuovi mercati decentralizzati per dati, potenza di calcolo e modelli, gestiti tramite token e DAO.

1 Introduzione

Intelligenza artificiale e blockchain sono tra i temi più discussi degli ultimi anni nell'ambito della tecnologia. Sviluppatisi in modo separato e rivolti verso obiettivi distinti, rispondono in realtà a bisogni complementari: la blockchain sostituisce la fiducia che normalmente viene riposta in operatori finanziari o fiduciari con la tracciabilità e la trasparenza; l'AI dal canto suo, introduce adattività su contenuti in linguaggi non formali e dati non strutturati, oltre a capacità predittiva e automazione dei processi. Insieme compongono un paradigma in cui i dati diventano verificabili e le decisioni automatiche possono essere certificate in modo immutabile. [27, 25, 12]

Questa convergenza non è né immediata nella dimostrazione di una qualsivoglia utilità pratica, né priva di sfide tecniche nel percorso di integrazione. Le due architetture partono da presupposti diversi: l'AI opera in modo statistico e tende alla centralizzazione delle risorse computazionali; la blockchain impone coerenza deterministica e governance distribuita, che normalmente viene identificata con "decentralizzazione". Comprendere queste differenze è il presupposto necessario per identificare dove l'integrazione produce valore reale e con quali strumenti tecnici può essere realizzata. [27, 25, 12]

De Cifris Koine – BITCOIN & BLOCKCHAIN
https://doi.org/10.69091/koine/vol-6-B09

Le direzioni in cui la convergenza si manifesta sono principalmente tre. La prima riguarda la certificazione dell'origine e dell'integrità dei dataset usati per addestrare i modelli AI — un problema di fiducia che la blockchain può contribuire ad affrontare, fornendo evidenze verificabili di integrità, provenienza e sequenza temporale. La seconda riguarda l'esecuzione di logiche intelligenti in smart contract. Questi ultimi loro malgrado denominati "smart" ma che in realtà sono stati finora caratterizzati da logiche molto poco intelligenti. La domanda che ci poniamo è se con lo sviluppo dell'AI anche gli smart contract potranno portare le capacità decisionali adattive nei sistemi on-chain, posto che questo non vada contro il cuore stesso dell'esecuzione di codice in blockchain, ossia la verificabilità.

La terza direzione apre alla creazione di nuovi mercati decentralizzati per dati, potenza di calcolo e modelli AI, gestiti tramite token e organizzazioni autonome decentralizzate (DAO).

Obiettivo di questo capitolo è analizzare ciascuna di queste direzioni con rigore tecnico, offrendo ai professionisti che operano in contesti eterogenei un quadro di riferimento utile a distinguere le applicazioni mature da quelle ancora in fase sperimentale.

2 Basi tecnologiche: architetture a confronto

Per comprendere come AI e blockchain possano integrarsi, è necessario partire dalle architetture di ciascuna tecnologia.

2.1 Blockchain: consenso, immutabilità, decentralizzazione

Le blockchain operano come registri distribuiti mantenuti da una rete di nodi che concordano sullo stato del sistema tramite meccanismi di consenso. A seconda del protocollo, il consenso può essere basato sul lavoro computazionale (Proof of Work), sulla partecipazione economica (Proof of Stake) o su altre forme di attestazione crittografica. [19]

Un'elevata resistenza alla modifica retroattiva deriva dalla struttura a catena: ogni blocco dipende crittograficamente dal precedente tramite una funzione hash. Alterare un dato registrato richiederebbe ricostruire l'intera catena controllando contestualmente la maggioranza del potere di consenso — una condizione economicamente o computazionalmente proibitiva nelle reti sufficientemente distribuite, pur senza escludere del tutto reorg, hard fork o interventi di governance. La decentralizzazione riduce la dipendenza da autorità centrali e distribuisce la responsabilità della verifica tra partecipanti indipendenti. [19]

Queste proprietà — riduzione della dipendenza da intermediari centrali, tracciabilità persistente, regole codificate e auto-eseguibili — costituiscono il contributo

strutturale della blockchain in un sistema integrato con l'AI. Va però osservato che la fiducia non viene eliminata, ma spostata su protocollo, client, validatori, oracoli, wallet e governance.

2.2 AI: modelli, dati e inferenza

L'intelligenza artificiale moderna si basa su modelli statistici addestrati su grandi volumi di dati, lungo un percorso che dalla preparazione dei dataset porta all'addestramento e infine all'inferenza — la produzione di output a partire da nuovi input.

I modelli di grandi dimensioni, come i Large Language Model (LLM) e le architetture di deep learning avanzate, richiedono infrastrutture ad alta capacità computazionale: cluster di GPU, pipeline di distribuzione ottimizzate, ambienti cloud specializzati. L'inferenza produce risposte probabilistiche: a parità di input, un modello può generare output leggermente diversi in funzione di parametri stocastici. Questa incertezza nel risultato finale è al tempo stesso il punto di forza dell'AI e la principale fonte di frizione quando i requisiti richiedono riproducibilità e determinismo. [26]

2.3 La sfida dell'integrazione: determinismo e adattività

La blockchain richiede determinismo: gli stessi input devono produrre sempre gli stessi output, affinché i nodi della rete raggiungano consenso, ma non solo. Ad esempio, un nuovo nodo che si unisce alla rete riceverà l'insieme di tutti i blocchi passati, a partire dal primo blocco di genesi, che esso dovrà processare e validare uno per uno in modo da ricostruire lo storico degli stati della rete ad ogni altezza di blocco.

Al contrario, l'AI introduce comportamenti adattativi e non deterministici per design. Questa differenza è la principale sfida tecnica da affrontare in qualsiasi architettura che integri le due tecnologie.

La soluzione adottata nella maggior parte dei sistemi esistenti è separare i livelli di esecuzione: l'AI opera off-chain, su infrastrutture dedicate, mentre la blockchain si occupa della registrazione degli input, della verifica delle condizioni contrattuali e dell'esecuzione delle conseguenze. Gli oracoli — componenti software che collegano la blockchain a sistemi esterni — svolgono il ruolo di ponte tra i due livelli.

Ricerche in corso esplorano soluzioni più avanzate, come i sistemi di verifiable computation e i proof-of-inference basati su Zero-Knowledge Proof (ZKP): tecniche crittografiche che consentono di dimostrare la correttezza di un calcolo senza rivelare i dati di input. Queste tecnologie aprono la prospettiva di una verifica on-chain delle inferenze AI, mantenendo la riservatezza dei dati e la separazione dei livelli computazionali. [4]

Nota: le Zero-Knowledge Proof sono già in uso in sistemi blockchain per la privacy delle transazioni (es. Zcash, zkSync) e per la scalabilità nei cosiddetti Roll-up, layer aggiuntivi che consentono di aumentare in modo significativo il throughput (numero di transazioni per unità di tempo) processabili dal sistema. L'applicazione delle Zero-Knowledge Proof alla verifica delle inferenze AI è oggetto di ricerca attiva con risultati promettenti, sebbene i costi computazionali rimangano elevati.

3 Convergenze tecniche: dove l'integrazione produce valore

Chiarite le architetture di base e le sfide dell'integrazione, è possibile analizzare in dettaglio i tre assi lungo i quali la convergenza tra AI e blockchain può essere esplorata e misurata. In ciascuno, la blockchain contribuisce con le sue proprietà di fiducia e immutabilità, mentre l'AI introduce adattività a dati non strutturati e capacità elaborativa.

3.1 Certificazione dell'origine e integrità dei dataset

La corruzione o manipolazione dei dataset di training rappresenta una vulnerabilità strutturale dei sistemi di machine learning. Tecniche di data poisoning possono alterare in modo mirato il comportamento del modello, introducendo backdoor o degradando le performance complessive; bias sistematici o selezioni distorte dei dati producono invece effetti meno visibili ma altrettanto critici, compromettendo robustezza, equità e affidabilità operativa. Anche l'assenza di tracciabilità delle fonti, di documentazione metodologica e di controlli di integrità riduce la possibilità di audit e di rilevazione di anomalie. In questo senso, la sicurezza del modello non è separabile dalla sicurezza e dalla governance del dato: l'integrità del training set costituisce un prerequisito tecnico per la resilienza del sistema.

La blockchain offre in questo contesto un registro immutabile per documentare la provenienza dei dataset. Ogni fase della data pipeline può essere registrata on-chain: acquisizione delle sorgenti, fasi di pulizia, trasformazioni applicate, versioni dei dataset, hash di integrità. Questo crea un audit trail riproducibile che impedisce modifiche non rilevate e rende verificabile la sequenza degli interventi effettuati prima dell'addestramento. [25, 12, 20]

L'ancoraggio della data pipeline su blockchain non implica che il codice o l'intero processo debbano essere open source: la tecnologia garantisce l'immutabilità e la verificabilità delle evidenze crittografiche registrate (hash, versioni, timestamp), non la trasparenza del contenuto sottostante. È quindi possibile mantenere proprietari codice e dataset, pubblicando on-chain solo le "impronte" digitali che ne attestano integrità e sequenza temporale. In questo schema, la blockchain non certifica la correttezza logica del processo, ma rende dimostrabile che determinati artefatti non

siano stati modificati dopo la loro registrazione, separando il tema della trasparenza da quello dell'immutabilità.

In contesti regolamentati — applicazioni mediche, finanziarie, giuridiche — questa capacità di audit ha valore diretto dal punto di vista della conformità normativa. Con l'entrata in vigore dell'AI Act europeo, la tracciabilità e la *data governance* dei dati di training per i modelli ad alto rischio diventano un requisito formale, non più una scelta opzionale. La blockchain può essere uno dei controlli tecnici utili a supportare gli obblighi di tracciabilità e documentazione, ma non sostituisce il sistema complessivo di governance, gestione del rischio, documentazione tecnica e conformità GDPR; l'AI Act, peraltro, resta tecnologicamente neutro e non impone alcuna tecnologia specifica, blockchain inclusa. [23]

Si consideri un esempio concreto. Un consorzio ospedaliero addestra un modello di supporto diagnostico su immagini radiologiche provenienti da cinque centri. Ogni centro, al momento del conferimento, registra on-chain l'hash del proprio lotto di dati, la data di acquisizione e la versione del protocollo di anonimizzazione applicato; le successive fasi di pulizia e normalizzazione vengono ancorate come transazioni distinte. Quando, a distanza di mesi, un'autorità di vigilanza chiede di dimostrare che il modello in produzione è stato addestrato solo su dati consentiti e non alterati, il consorzio non deve produrre dichiarazioni autocertificate: esibisce l'audit trail, e chiunque può ricalcolare gli hash dei dataset e verificarne la corrispondenza con quanto registrato. La proprietà delle immagini resta riservata — on-chain figurano solo le impronte crittografiche — ma la sequenza degli interventi diventa verificabile in modo indipendente, contribuendo a soddisfare l'obbligo di tracciabilità previsto dall'AI Act per i sistemi ad alto rischio. [23] Va però osservato che, in contesti sanitari, anche hash, timestamp, dimensione del lotto e metadati devono essere progettati per evitare rischi di correlazione o re-identificazione: su dataset piccoli, rari o facilmente collegabili sono in alcuni casi preferibili *commitment* con *salting*, registri *permissioned* o attestazioni off-chain.

3.2 Logiche intelligenti in smart contract e agenti autonomi

Nelle blockchain programmabili uno smart contract è rappresentato on-chain almeno dal proprio bytecode eseguibile e dal relativo stato; il codice sorgente può essere pubblicato e verificato tramite strumenti esterni, ma non coincide necessariamente con ciò che la blockchain registra direttamente. Ad ogni transazione che li coinvolge sono inoltre registrati gli input e gli eventuali cambiamenti di stato. Essi in genere implementano le logiche di un accordo quando certe condizioni vengono soddisfatte. Integrarli con capacità AI aprirebbe la possibilità di decisioni contrattuali adattive, basate su dati non strutturati piuttosto che su regole fisse predefinite.

L'architettura tipica prevede che lo smart contract registri l'input che origina la richiesta, il quale a sua volta viene trasmesso verso un modello AI off-chain

tramite un oracolo — l'infrastruttura che osserva fonti esterne, elabora o aggrega dati off-chain e li pubblica su smart contract consultabili dal protocollo, e che nelle architetture reali può assumere la forma di una rete di nodi, feed e meccanismi di aggregazione anziché di un singolo processo. Ricevuto il risultato dell'inferenza vengono applicate le conseguenze contrattuali in modo automatico e verificabile. Questo schema è già in uso in alcuni sistemi DeFi (Decentralized Finance) per la valutazione del rischio e la gestione dinamica delle posizioni.

Un caso già operativo aiuta a fissare il meccanismo. Nei protocolli di lending come Aave o Compound III, le posizioni degli utenti sono garantite da collaterale e diventano liquidabili quando il rapporto tra debito e valore della garanzia supera una soglia definita a livello di protocollo — espressa in Aave come *Health Factor* inferiore a 1 e in Compound III come superamento del *liquidation collateral factor*. La liquidazione è *permissionless*: attori esterni (i cosiddetti *liquidator*, tipicamente bot) monitorano off-chain prezzi e stato delle posizioni e, non appena la soglia risulta superata, sottomettono on-chain la transazione di liquidazione, che lo smart contract esegue solo dopo aver verificato la condizione in modo deterministico tramite un oracolo di prezzo — in entrambi i protocolli, oggi, i Chainlink Price Feed come fonte primaria. [1, 11, 10] Nella prassi attuale questi bot sono *trigger* deterministici basati su soglia, e la competizione tra liquidatori si gioca sulla velocità di esecuzione e su dinamiche di tipo MEV, non su modelli predittivi. L'impiego di componenti di intelligenza artificiale — per anticipare quali posizioni stanno per diventare liquidabili o per ottimizzare la strategia di esecuzione — rappresenta una direzione di ricerca e un'estensione possibile, non un elemento del meccanismo *core*: la decisione di liquidazione resta una verifica on-chain regola-deterministica fondata sul prezzo dell'oracolo.

Un passo ulteriore sarebbe rappresentato dagli agenti autonomi on-chain: sistemi software che combinano capacità decisionali AI con la possibilità di eseguire transazioni blockchain in modo indipendente. Questi agenti possono operare in mercati decentralizzati, gestire risorse digitali o coordinarsi con altri agenti, aprendo scenari di automazione complessa con tracciabilità nativa di ogni azione.

Tuttavia, l'attuale modello di calcolo su cui sono basati gli smart contract nelle reti più popolari come ad esempio Ethereum, è caratterizzato dalla necessità di eseguire il loro codice in modo ridondato in tutti i nodi della rete. Ciò impone la frugalità nell'uso delle risorse del nodo locale e ciò non sembra favorire lo sviluppo di algoritmi complessi ed esecuzione di inferenza direttamente on-chain.

3.3 Certificazione dell'origine dei modelli e verificabilità

In un ecosistema in cui i modelli AI vengono distribuiti, modificati, ri-addestrati e condivisi, verificare l'autenticità e la versione di un modello è un problema non

banale. La blockchain può ancorare hash crittografici dei pesi, dei parametri e dei metadati di un modello, consentendo a chiunque di verificare in modo indipendente che il modello utilizzato corrisponda a quello dichiarato.

Questo è particolarmente rilevante per modelli distribuiti, open-source o sviluppati collaborativamente, dove la provenienza e la coerenza delle versioni diventano critiche per la sicurezza. In sistemi di federated learning — in cui più organizzazioni contribuiscono all'addestramento di un modello comune senza condividere i propri dati — la blockchain può fornire un meccanismo neutrale di registrazione e verifica dei contributi di ciascun partecipante.

Per le singole inferenze, i proof-of-inference basati su Zero-Knowledge Proof rappresentano una frontiera tecnica che consentirebbe di certificare la correttezza di un'inferenza senza rivelare né i dati di input né i pesi del modello. La combinazione di autenticità del modello e verificabilità dell'inferenza costituisce la base tecnica per sistemi AI certificati e auditabili per design. [4]

Per rendere tangibile la nozione di proof-of-inference, si consideri un servizio che offre uno *scoring* creditizio tramite un modello proprietario. Il cliente vuole la garanzia che il punteggio ricevuto sia stato prodotto da quel modello specifico, e non da una versione scadente o manomessa; il fornitore, però, non può rivelare né i pesi del modello né i dati dell'istruttoria. Con le tecniche di *Zero-Knowledge Machine Learning* (ZKML) il fornitore allega all'output una prova crittografica che attesta: "questo punteggio è il risultato dell'esecuzione del modello il cui hash è registrato on-chain, applicato a un input valido", senza divulgare altro. Sul piano implementativo, la libreria open-source *EZKL* consente di generare prove zk-SNARK a partire da modelli in formato ONNX [28], lungo un filone aperto da contributi fondativi come il benchmark *The Cost of Intelligence* di Modulus Labs [18]. La maturità resta tuttavia limitata: la generazione della prova è praticabile per reti di dimensioni medie, ma ancora proibitiva per i modelli linguistici di grande scala. Il caso mostra comunque concretamente cosa significhi "certificare un'inferenza" al di là dell'enunciato teorico. [4] È bene precisare la portata di questa garanzia: la prova attesta che un certo calcolo è stato eseguito correttamente rispetto a un modello, un input e dei parametri impegnati crittograficamente, ma non prova che l'output sia vero, equo, giuridicamente corretto o sostanzialmente adeguato al caso d'uso.

Vale la pena soffermarsi su una proprietà spesso evocata nel dibattito sulla computazione intelligente: l'*additività*. La computazione intelligente designa un campo ampio — reti neurali, logica fuzzy, algoritmi evolutivi, apprendimento automatico — mentre l'additività è una proprietà matematica che solo *alcuni* modelli possiedono: un modello è additivo quando il suo risultato si decompone nella somma di contributi separati delle singole variabili, come negli *additive model* o nei *generalised additive model*. Lo *scoring* creditizio dell'esempio precedente è additivo se espresso come $r = f_1(x_1) + f_2(x_2) + f_3(x_3)$, dove f_1, f_2 e f_3 isolano l'effetto di reddito, età e indebitamento come contributi indipendenti.

L'additività è rilevante in due sensi distinti, che conviene non confondere. Sul piano *interpretativo*, i modelli additivi consentono di isolare il contributo di ciascuna variabile e risultano perciò più facilmente auditabili — una proprietà preziosa per la verificabilità di cui si è discusso. Va però evitata un'estensione indebita: la preattivazione di un singolo neurone, $z = w_1x_1 + \cdots + w_nx_n + b$, è sì una somma pesata, ma le non linearità e la composizione di molti strati fanno sì che una rete neurale, nel suo complesso, *non* sia additiva né interpretabile in questo senso. I modelli più espressivi introducono per costruzione interazioni tra variabili, in cui l'effetto congiunto di due fattori eccede la somma dei loro effetti separati.

Sul piano *distribuito*, molte procedure di apprendimento federato aggregano gli aggiornamenti locali dei partecipanti mediante somme o medie pesate: questa struttura additiva si presta a tecniche di *secure aggregation* o di crittografia omomorfica, che permettono di calcolare la somma anche su contributi cifrati. I due piani, tuttavia, non coincidono: un'aggregazione additiva degli aggiornamenti non rende automaticamente interpretabile né auditabile il modello risultante. La scelta tra modelli additivi e modelli con interazioni resta così, in un'architettura che integra AI e blockchain, un compromesso tra trasparenza verificabile e potere espressivo.

Sul versante della ricerca, proposte architetturali recenti tentano di formalizzare questi requisiti in framework completi. Palliora [8, 7], ad esempio, organizza la computazione verificabile e confidenziale attorno a una rete di attori specializzati — *guardians* che mediano l'accesso ai dati, *calculators* che eseguono il calcolo con livelli di confidenzialità variabili e *verifiers* che ne attestano la correttezza di input e output — coordinati da *computable contracts* su una blockchain dedicata, ed è pensata esplicitamente per scenari AI quali modelli cifrati, marketplace e agenti verificabili. Allo stato attuale si tratta di una proposta accademica con implementazione prototipale (la testnet *Manas*), priva di token pubblico, mainnet o adozione di mercato comparabile a quella dei protocolli discussi nel seguito.

3.4 Un rovesciamento di prospettiva: l'AI nell'analisi dei protocolli

Le tre direzioni esaminate finora descrivono la blockchain come infrastruttura di fiducia al servizio dell'AI. Nel 2026 la convergenza ha però mostrato con forza il verso opposto: i modelli generativi di frontiera sono diventati strumenti capaci di analizzare protocolli e sistemi in produzione e di individuare vulnerabilità che anni di revisione umana non avevano colto.

L'esempio più pertinente al nostro tema è emerso nel maggio 2026. Durante un audit del protocollo Zcash commissionato da Shielded Labs, il ricercatore Taylor Hornby, assistito dal modello Opus 4.8, ha individuato un difetto di *soundness* nel circuito Orchard — il principale *shielded pool* della rete. Il difetto, un vincolo di uguaglianza mancante nella moltiplicazione scalare del circuito, permetteva di forgiare i *nullifier* e coniare quantità illimitate di ZEC contraffatto; in un sistema in cui i saldi sono nascosti per costruzione, una contraffazione non rilevabile è prossima

allo scenario peggiore. Il difetto era presente fin dal lancio di Orchard, nel maggio 2022, ed era sfuggito ad audit precedenti condotti con modelli meno recenti. La gestione è stata esemplare: nessuno sfruttamento on-chain, segnalazione responsabile e correzione in pochi giorni tramite un *soft fork* d'emergenza che ha disabilitato Orchard e, il giorno successivo, l'*hard fork* di rete NU6.2 con il circuito corretto. [6, 13]

Lo stesso anno ha reso evidente l'altra faccia della medaglia. Le capacità offensive di questi modelli hanno raggiunto un livello tale da motivare un intervento regolatorio senza precedenti: nel giugno 2026, secondo quanto riportato dalla stampa, il governo statunitense ha limitato l'accesso ai modelli Mythos e Fable di Anthropic da parte di cittadini stranieri per ragioni di sicurezza nazionale, inducendo l'azienda a disabilitarli globalmente prima di concederne un rilascio controllato a un ristretto numero di partner — in quello che è stato indicato come il primo caso di controlli all'esportazione applicati a un modello di AI anziché al solo hardware. [15] Modelli del fronte commerciale, come GPT-5.5, sono stati classificati dai rispettivi sviluppatori come dotati di capacità di cybersecurity "elevate". [21]

Questi episodi convergono su una considerazione che riguarda direttamente le architetture discusse in questo capitolo. Lo stesso strumento può servire tanto il difensore quanto l'attaccante, e la finestra fra la scoperta responsabile di una falla e il suo possibile sfruttamento si assottiglia man mano che l'analisi assistita da AI diventa più potente e accessibile. I circuiti a conoscenza zero su cui poggiano la verificabilità delle inferenze e la riservatezza delle transazioni sono essi stessi software, esposti a questa analisi: una garanzia di robustezza quando è in mani difensive, un rischio quando non lo è. La sicurezza dei sistemi che integrano AI e blockchain non può quindi considerarsi acquisita una volta per tutte, ma va riverificata alla luce di strumenti di analisi in rapida evoluzione.

4 Mercati decentralizzati: dati, calcolo e modelli AI

La convergenza tra AI e blockchain non si esaurisce nella certificazione dei dati e nell'integrazione tecnica tra sistemi: apre anche la possibilità di nuovi modelli economici decentralizzati. I token e le DAO — Decentralized Autonomous Organizations — costituiscono gli strumenti con cui incentivare, gestire e governare mercati distribuiti di dati, potenza di calcolo e modelli AI, senza ricorrere a intermediari centralizzati.

Questa dimensione è la più recente e la più sperimentale tra quelle trattate in questo capitolo. I progetti esistenti mostrano sia il potenziale sia i limiti di questi meccanismi: alcune architetture hanno dimostrato funzionare a scala, altre sono rimaste nel dominio della ricerca o hanno fallito nell'allineamento tra incentivi economici e qualità tecnica. Analizzarli con rigore è necessario per distinguere l'innovazione strutturale dalla sperimentazione ancora in corso.

4.1 Token come strumenti di incentivo economico

Diversamente dalle criptovalute native di una rete — come Ether su Ethereum o bitcoin su Bitcoin — un *token* emesso e gestito tramite smart contract è programmabile, e può quindi rappresentare diritti di accesso, quote di governance, ricompense per contributi o partecipazione ai ricavi di un protocollo. Tre categorie sono rilevanti per i mercati AI decentralizzati.

Gli *utility token* danno accesso a un servizio o a una risorsa del protocollo: pagare un'inferenza, acquistare un dataset, accedere alla potenza di calcolo di una rete distribuita.

I *governance token* attribuiscono potere di voto sulle decisioni che la community assume su un protocollo, come ad esempio: parametri tecnici, aggiornamenti, criteri di ammissione dei contributori.

I *reward token* vengono distribuiti automaticamente come ricompensa per contributi verificabili — dataset validati, risorse computazionali messe a disposizione, aggiornamenti approvati a un modello condiviso.

Applicati all'AI, i meccanismi tokenomici affrontano un problema fondamentale: come remunerare equamente la produzione di dati di qualità. I dati sono asimmetrici per natura — chi li detiene ha difficoltà a dimostrarne il valore senza rivelarli, e chi li acquista non può valutarli pienamente prima dell'acquisto. Protocolli come Ocean Protocol affrontano questa asimmetria con il modello compute-to-data: invece di trasferire i dati al compratore, l'algoritmo viene portato dove risiedono i dati, che non lasciano mai il controllo del proprietario. Il token OCEAN remunera la fornitura di dati e di capacità di calcolo all'interno dell'ecosistema; va peraltro ricordato che Ocean Protocol ha aderito nel 2024 alla *Artificial Superintelligence Alliance* — la fusione con Fetch.ai e SingularityNET, con conversione dei rispettivi token in FET/ASI — per poi uscirne nell'ottobre 2025, ripristinando OCEAN come token indipendente. [20, 3]

Un secondo ambito riguarda la potenza di calcolo. Reti come Render Network e Akash consentono a chiunque di mettere a disposizione risorse GPU o CPU in cambio di token, creando un mercato decentralizzato di infrastruttura computazionale alternativo ai grandi cloud provider. Il pricing è determinato dalla domanda e dall'offerta on-chain, con meccanismi di reputazione per i fornitori che garantiscono livelli di servizio verificabili. [24, 2]

I limiti di questi meccanismi sono reali. La volatilità dei token introduce incertezza nei flussi di ricavo per i contributori, disincentivando la partecipazione a lungo termine. Il pricing equo per risorse eterogenee — un dataset di immagini mediche rare ha un valore completamente diverso da un dataset di testi generici — è un problema aperto, che i meccanismi di mercato da soli non risolvono. Infine, la speculazione sul

valore dei token può distorcere gli incentivi, spingendo i contributori a ottimizzare il guadagno a breve termine piuttosto che la qualità del contributo.

4.2 DAO come strutture di governance per l'AI

Una DAO è un'organizzazione le cui regole sono codificate in smart contract sulla blockchain ed eseguite automaticamente senza bisogno di un'autorità centrale, almeno in teoria. Le decisioni vengono prese tramite voto on-chain dei detentori di governance token: proposte, delibere e implementazioni seguono un processo trasparente, registrato e auditabile. Applicate all'AI, le DAO offrono una risposta alla domanda su chi debba controllare i modelli condivisi e come debbano essere prese le decisioni sui loro aggiornamenti. [9] Va però osservato che la decentralizzazione delle DAO è spesso parziale: nella pratica molte dipendono comunque da fondazioni, multisig, core team, delegati o gruppi tecnici con poteri di intervento rapido.

SingularityNET è uno degli esempi più avanzati in questo spazio: una piattaforma decentralizzata in cui agenti AI sviluppati da terze parti possono essere pubblicati, scoperti e remunerati, con governance affidata a una DAO. Il suo token originario AGIX è confluito nel token FET/ASI con la già citata Artificial Superintelligence Alliance (2024); il marketplace dei servizi AI continua a operare regolando i pagamenti in tale token. [16, 3] Bittensor adotta un approccio diverso: crea un mercato competitivo in cui i contributori (*miner*) erogano servizi di intelligenza — non solo modelli linguistici, ma diversi compiti di machine learning organizzati in *subnet* — mentre un insieme di *validator* ne valuta continuamente la qualità; il meccanismo di consenso *Yuma* aggrega tali giudizi pesandoli per la posta in gioco (*stake*) e distribuisce i token TAO ai contributori giudicati più utili. [5]

La governance DAO consente di distribuire automaticamente i ricavi generati da un modello AI tra tutti i contributori — dati, calcolo, sviluppo — proporzionalmente al contributo verificato on-chain. Questo elimina la necessità di intermediari che gestiscano i pagamenti e rende il processo di distribuzione trasparente e contestabile. Gli smart contract possono anche codificare regole di priorità — ad esempio, reinvestire una quota dei ricavi in ricerca o in compensazioni per i contributori originali di dataset.

I limiti della governance decentralizzata non vanno sottovalutati. La partecipazione effettiva ai voti è strutturalmente bassa nella maggior parte delle DAO esistenti [14]: la complessità tecnica delle proposte scoraggia i detentori di token non specializzati, e le decisioni finiscono per essere influenzate da una minoranza di partecipanti attivi. La concentrazione del potere di voto — quando grandi detentori di token controllano de facto le delibere — riproduce dinamiche centralizzate in una struttura formalmente distribuita. La lentezza del processo decisionale, infine, rende le DAO inadatte a rispondere rapidamente a vulnerabilità tecniche o a cambiamenti rapidi del contesto competitivo.

4.3 Mercati decentralizzati di dati e modelli

L'insieme di token, smart contract e DAO costituisce l'infrastruttura su cui si costruiscono mercati decentralizzati specifici per l'AI: marketplace di dataset, di potenza di calcolo e di modelli addestrati. Questi mercati condividono una caratteristica comune: separare la proprietà della risorsa dalla possibilità di utilizzarla, senza richiedere il trasferimento fisico del dato o del modello a chi ne fa uso.

Il paradigma compute-to-data — introdotto da Ocean Protocol e adottato in forma diverse da altri protocolli — inverte la logica tradizionale: invece di inviare i dati all'algoritmo, l'algoritmo viene eseguito nell'ambiente del proprietario dei dati. Il risultato dell'elaborazione viene restituito senza che il dataset lasci mai il controllo di chi lo detiene. Questo approccio è particolarmente rilevante per dati sensibili — sanitari, finanziari, personali — in cui la condivisione diretta sarebbe incompatibile con il GDPR o con obblighi di riservatezza contrattuale. Il compute-to-data può ridurre l'esposizione del dato e facilitare architetture privacy-preserving, ma non elimina gli obblighi GDPR: base giuridica, ruoli privacy, DPIA, minimizzazione, sicurezza, trasferimenti e diritti degli interessati restano comunque necessari. [20, 17]

I marketplace di modelli AI funzionano secondo una logica analoga: un modello addestrato viene registrato on-chain tramite hash crittografico, le condizioni di utilizzo e i meccanismi di remunerazione vengono codificati in uno smart contract, e ogni accesso al modello genera automaticamente una royalty distribuita ai creatori secondo le regole definite. Questo consente a ricercatori e organizzazioni di monetizzare modelli proprietari senza cederli, e a chi li utilizza di verificarne l'autenticità e la versione in modo indipendente.

L'interoperabilità tra marketplace diversi è ancora un problema aperto. La maggior parte dei protocolli esistenti opera in ecosistemi chiusi, con token e standard incompatibili. Iniziative come il progetto AI Alliance e alcuni working group legati a Ethereum stanno lavorando a standard condivisi per la portabilità dei modelli e l'interoperabilità dei marketplace, ma siamo ancora in una fase di frammentazione.

Sul piano regolatorio, i mercati decentralizzati di dati e modelli AI si collocano in una zona di sovrapposizione tra normative diverse: il GDPR per i dati personali, le norme sulla proprietà intellettuale per i modelli addestrati, e potenzialmente le normative sui mercati finanziari per i token che incorporano diritti economici. L'AI Act europeo introduce ulteriori requisiti per i modelli ad alto rischio, inclusi obblighi di tracciabilità e documentazione che i marketplace decentralizzati dovranno integrare nelle proprie architetture per operare in conformità. [22, 23]

Il panorama attuale è eterogeneo. Alcuni protocolli — in particolare Bittensor, con oltre cento *subnet* attive, e Render Network, con volumi di rendering dell'ordine di milioni di frame — hanno raggiunto una scala operativa reale e comunità di contributori attive; conviene tuttavia distinguere l'attività realmente produttiva

dalla capitalizzazione di mercato dei rispettivi token, che riflette anche dinamiche speculative. Altri hanno fallito per disallineamento tra incentivi economici e qualità tecnica, o per incapacità di attrarre massa critica. La lezione principale dai casi di insuccesso è che la tokenomics non può sostituire la qualità del prodotto: un marketplace decentralizzato funziona solo se i dati o i modelli che vi transitano hanno valore intrinseco, indipendentemente dai meccanismi di incentivo. [20, 24, 5]

Nota: il termine 'tokenomics' indica il sistema economico di un protocollo blockchain — la distribuzione, l'emissione, la domanda e l'utilità dei token. La progettazione della tokenomics è una disciplina ibrida tra economia, teoria dei giochi e ingegneria dei protocolli, con impatto diretto sulla sostenibilità a lungo termine di un ecosistema decentralizzato.

5 Conclusioni

AI e blockchain non sono tecnologie destinate a restare separate. Le loro differenze architetturali — che a prima vista sembrano ostacoli — si rivelano complementarità: laddove l'AI introduce flessibilità e capacità predittiva, la blockchain fornisce la struttura di fiducia necessaria a rendere quelle capacità verificabili e responsabili.

I quattro assi di convergenza analizzati in questo capitolo mostrano gradi diversi di maturità. La certificazione dei dati di training e la certificazione crittografica dei modelli sono le direzioni più consolidate, con architetture definite e casi d'uso reali già in produzione. L'orchestrazione di logiche AI tramite smart contract è in rapida evoluzione, trainata dall'adozione nei mercati DeFi. I mercati decentralizzati di dati, calcolo e modelli — governati da token e DAO — sono il fronte più ambizioso e sperimentale: alcuni protocolli hanno dimostrato funzionare a scala, ma la categoria nel suo insieme è ancora in fase di consolidamento, con sfide aperte sul piano tecnico, economico e regolatorio.

Per i professionisti che operano in contesti regolamentati, la convergenza tra AI e blockchain offre strumenti concreti per rispondere a requisiti emergenti di trasparenza e auditabilità — in particolare nel quadro dell'AI Act europeo. Per chi lavora nell'innovazione tecnologica, apre scenari di progettazione che superano i limiti dei sistemi centralizzati tradizionali. Per i crittografi, infine, introduce nuove frontiere di ricerca — dai proof-of-inference alle ZKP applicate all'AI — in cui le basi matematiche della crittografia diventano il fondamento della fiducia nei sistemi AI.

References

1. Aave. Aave protocol documentation: Liquidations, 2024.
2. Akash Network. Akash: A decentralized cloud computing marketplace, 2020. Whitepaper.

3. Artificial Superintelligence Alliance. ASI token merger: Fetch.ai, SingularityNET and ocean protocol, 2024.
4. E. Ben-Sasson et al. Succinct non-interactive arguments for a von Neumann architecture. In *Advances in Cryptology — CRYPTO 2013*, 2013. IACR ePrint 2013/879.
5. Bittensor Foundation. Bittensor: A peer-to-peer intelligence market, 2022. Whitepaper.
6. BlockSec. Zcash orchard soundness bug analysis. Security analysis, 2026.
7. C. Brunetta, A. Chaudhary, S. Galatolo, and M. Sala. An approach to computable contracts with verifiable computation outsourcing and blockchain transactions, 2025. IACR Cryptology ePrint Archive, Paper 2025/1896.
8. C. Brunetta, A. Chaudhary, S. Galatolo, and M. Sala. Palliora: A decentralized platform for sharing intelligent thoughts. Technical report, ShunyaXifra, 2026. White paper, Version 1.1.
9. V. Buterin. DAOs, DACs, DAs and more: An incomplete terminology guide. Ethereum Blog, 2014.
10. Chainlink. Chainlink price feeds documentation, 2024.
11. Compound. Compound iii documentation: Liquidation, 2024.
12. T.N. Dinh and M.T. Thai. AI and blockchain: A disruptive integration. *IEEE Computer*, 51(9):48–53, 2018.
13. Electric Coin Company and Zcash Open Development Lab. Zcash NU6.2 network upgrade: Orchard circuit fix. Release notes, 2026.
14. B. Falk, T. Pathan, A. Rigas, and G. Tsoukalas. Blockchain governance: An empirical analysis of user engagement on DAOs, 2024.
15. Fortune. Anthropic disables fable and mythos AI models following U.S. government export ban, 2026.
16. B. Goertzel et al. SingularityNET: A decentralized, open market and network for AIs, 2023. Whitepaper.
17. T. McConaghy. Ocean protocol: Tools for the Web3 data economy. In *Handbook on Blockchain*, volume 194 of *Springer Optimization and Its Applications*. Springer, 2022.
18. Modulus Labs. The cost of intelligence: Proving machine learning inference with zero-knowledge, 2023.
19. S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008.
20. Ocean Protocol Foundation. Ocean protocol: A decentralized substrate for AI data & services, 2022. Whitepaper v4.
21. OpenAI. GPT-5.5 system card, 2026.
22. Parlamento europeo e Consiglio dell'Unione europea. Regolamento (UE) 2016/679 — regolamento generale sulla protezione dei dati (GDPR). Technical report, Gazzetta Ufficiale dell'Unione europea, 2016.
23. Parlamento europeo e Consiglio dell'Unione europea. Regolamento (UE) 2024/1689 — artificial intelligence act. Technical report, Gazzetta Ufficiale dell'Unione europea, 2024.
24. Render Network Foundation. The render network: Distributed GPU rendering on the blockchain, 2023. Whitepaper.
25. K. Salah, M.H.U. Rehman, N. Nizamuddin, and A. Al-Fuqaha. Blockchain for AI: Review and open research challenges. *IEEE Access*, 7:10127–10149, 2019.
26. A. Vaswani et al. Attention is all you need. In *Advances in Neural Information Processing Systems (NeurIPS)*, 2017.

27. L. Witt, A.T. Fortes, K. Toyoda, W. Samek, and D. Li. Blockchain and artificial intelligence: Synergies and conflicts, 2024.
28. Zkonduit. EZKL: Zero-knowledge proofs for machine learning models. Software library, 2024.

Part IV
Aspetti Legali

La disciplina delle cripto-attività nell'UE e nel Regno Unito: Scenari Regolatori a Confronto

Cristina Poncibò[1] and Luigi Cantisani[2]

[1] Università di Torino, Italy
cristina.poncibo@unito.it
[2] University of Warwick, United Kingdom
luigi.cantisani@warwick.ac.uk

Abstract. Il 2025 ha segnato un momento di svolta nella regolamentazione delle cripto-attività. Nell'UE, l'entrata a pieno regime del Regolamento sui mercati delle cripto-attività (MiCA) ha introdotto un quadro normativo rigoroso, con requisiti di autorizzazione stringenti per le aziende che forniscono servizi legati alle cripto, che stanno già escludendo dal mercato alcuni operatori, incluse numerose aziende precedentemente legittimate ad operare sulla base della mera conformità alle leggi antiriciclaggio. Si passa quindi ad un regime per vere e proprie attività finanziarie regolate e vigilate. Attualmente, MiCA disciplina le attività degli emittenti di stablecoin e di una serie di prestatori di servizi per cripto-attività. Mentre l'UE attraversa la fase di implementazione del MiCA, il Regno Unito ha nel corso del 2025 proposto il proprio regime regolatorio, che appare più ampio e potrebbe complicare ulteriormente le operazioni transfrontaliere post-Brexit per le fintech britanniche. L'articolo quindi un'analisi comparata delle principali questioni regolatorie che andranno a caratterizzare l'industria delle cripto-attività negli anni a venire.

1 Introduzione

Il 2025 sarà probabilmente ricordato nel panorama regolatorio europeo relativo alle cripto-attività per due sviluppi fondamentali: l'entrata in vigore, in tutta l'Unione Europea (UE), del Regolamento (UE) 2023/1114 relativo ai mercati delle cripto-attività (MiCA) e la pubblicazione delle prime proposte di regolamentazione del nuovo regime regolatorio di tali attività nel Regno Unito sotto il Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (RAO).

Non vi è dubbio che il quadro normativo dell'UE, basato su un modello autorizzativo rigoroso e su requisiti di autorizzazione stringenti e vigilanza continuativa da parte delle autorità di supervisione dei mercati finanziari, stia già rimodellando il

De Cifris Koine – BITCOIN & BLOCKCHAIN
https://doi.org/10.69091/koine/vol-6-B10

mercato, escludendo gli operatori le cui attività non risultino essere conformi alla disciplina del regolamento. A titolo esemplificativo, delle oltre centocinquanta piattaforme di servizi per asset virtuali registrate in Italia secondo il precedente regime antiriciclaggio (AML), tipicamente *centralised exchange* (CEX) e wallet provider,[3] nessuna ha ancora in poche hanno ottenuto autorizzazioni MiCA per operare come prestatore di servizi (CASP) sotto il nuovo regime.[4] Una situazione analoga si osserva in Lituania, dove più di trecento VASP erano precedentemente autorizzate, ma attualmente solo sei società hanno ottenuto l'autorizzazione secondo il nuovo e più rigoroso regime MiCA. Inoltre, al momento della stesura, anche Binance, il più grande CEX cripto al mondo per quota di mercato, non ha ottenuto l'autorizzazione MiCA alla data di consegna di questo articolo.

Considerazioni similari si valgono anche per gli emittenti di stablecoin. MiCA introduce requisiti stringenti sulle riserve a supporto delle stablecoin, volti a mitigare il rischio di de-pegging,[5] e limita l'emissione di stablecoin riferite a valute ufficiali, gli *electronic money token* (EMT) alle entità già autorizzate come istituti di credito (cioè banche) o istituti di moneta elettronica (IMEL). Un trattamento differente si applica alle stablecoin riferite a un paniere di asset, che sarà discusso più avanti in questo articolo. In tale contesto, gli attori principali, come Tether, hanno abbandonato il mercato dell'UE, con la rimozione di USDT da parte dei CASP.

Le difficoltà autorizzatorie sono dovute ad una serie di requisiti stringenti, tra cui una comprovata esperienza finanziaria e manageriale dei dirigenti, una reale presenza operativa all'interno dell'UE supportata da personale locale qualificato e un'attenzione elevata alla cybersecurity e alla resilienza operativa. Per gli emittenti di stablecoin si aggiunge la già sopra menzionata questione della disponibilità di asset sottostanti in gradi di garantire la stabilizzazione. Non solo, i sottostanti devono essere altamente liquidi per consentire agli utenti di esercitare il *redemption right* e riconvertire gli stablecoin in valuta ufficiale a richiesta.

Per i soggetti interessati ad operare in tutto il continente europeo, abbracciando anche il Regno Unito, la questione potrebbe diventare presto più complessa. Il progetto di regolamento britannico sulle cripto-attività, arrivando dopo, sembra essersi preso il tempo per catturare e disciplinare nel proprio ambito di applicazione una gamma di servizi ed entità potenzialmente più ampia, sollevando questioni su

[3] Qui i due termini sono utilizzati secondo il significato tipico del gergo del settore, per indicare chi fornisce servizi di scambio e account o portafogli di custodia cripto dove il provider conserva le chiavi crittografiche necessarie a firmare le transazioni. Le categorie legali in senso tecnico sono trattate invece nel prosieguo

[4] L'elenco delle aziende ad oggi autorizzate è consultabile direttamente dal registro pubblico dell'ESMA, accessibile da: `https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica#InterimMiCARegister`.

[5] Cioè il rischio che lo stablecoin non abbia davvero asset sottostanti in misura adeguata a garantire la stabilità del valore.

come gestire filiali UE e filiali UK che potrebbero trovarsi disallineate in termini di autorizzazioni e percorsi di *compliance.*

Questo contributo non intende fornire un'analisi tecnica dettagliata di MiCA né della proposta regolatoria britannica, anche perché quest'ultima è composta al momento di sole bozze: uno *statutory instrument* non ancora approvato dal Parlamento, che andrebbe ad espandere il *Financial Securities and Markets Act*, ossia il Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (RAO), a cui si accompagnerà la regolamentazione di secondo livello della *Financial Conduct Authority* (FCA) in consultazione pubblica. Lo scopo di questo lavoro è quindi piuttosto quello di offrire una panoramica preliminare comparativa volta ad evidenziare le sfide operative per le aziende pan-europee.

2 Regolamento MiCA: Cenni Introduttivi

MiCA rappresenta il primo tentativo di regolamentazione dei mercati di cripto-attività armonizzata a livello europeo direttamente applicabile in tutti gli Stati Membri, con l'obiettivo di fornire certezza giuridica per specifiche categorie di token crittografici basati su tecnologia DLT. Questo Regolamento introduce un quadro normativo basato sul rischio, secondo il quale le attività sono classificate e soggette a trattamenti regolatori differenziati. Esso impone rigorosi requisiti di autorizzazione e supervisione prudenziale su determinati emittenti, nonché sugli intermediari che forniscono servizi correlati a tali asset. Centrale in questo quadro è il concetto di "cripto-attività", definito formalmente dal Regolamento come una rappresentazione digitale di valore o diritti che possono essere trasferiti e conservati elettronicamente utilizzando tecnologia a registro distribuito (DLT) o sistemi decentralizzati equivalenti.[6]

L'applicabilità di MiCA si valuta quindi in prima battuta sulla valutazione giuridica dell'asset oggetto di offerta al pubblico, ammissione a negoziazione o della prestazione di servizi. Quando un asset non è né legalmente fungibile né trasferibile, esso perde rilevanza per MiCA, cadendo quindi al di fuori del suo ambito. Al contrario, se queste caratteristiche fondamentali sono presenti, occorre procedere a un'ulteriore distinzione: se il token ha caratteristiche giuridiche che lo rendono un equivalente di classi d'asset tradizionali come, ad esempio, azioni, obbligazioni, e derivati (nel prosieguo, per brevità, indicheremo queste categorie tradizionali come "TradFi Asset Class"), esso rimane soggetto alle norme dell'UE pre-esistenti, e non rientra nel perimetro di MiCA. L'attenzione verte dunque per intero sulla natura giuridica sostanziale del token piuttosto che sulla tecnologia sottostante utilizzata per la sua emissione o circolazione.

Laddove, invece, un token crittografico, fungibile e negoziabile, non rientri in alcuna delle TradFi Asset Class, esso viene catturato da MiCA. I token catturati

[6] Definizione giuridica contenuta nell'Art. 3.1(5) del MiCA.

da MiCA si dividono in tre sottocategorie. La prima comprende gli *asset-referenced token* (ART), cioè quei token che puntano a mantenere un valore stabile facendo riferimento a altro valore o diritto, o a una combinazione di essi, comprese una o più valute ufficiali (ad esempio, uno stablecoin ancorato al valore dell'oro).[7]

La seconda categoria consiste dei già accennati EMT, la tipologia più in uso di stablecoin, i quali stabilizzazione il proprio valore attraverso l'ancoraggio ad una valuta ufficiale.[8] In altre parole, si tratta del mezzo per avere un "duplicato" on-chain dell'euro, dollaro, o qualunque altra valuta ufficiale che ad oggi non viene battuta ufficialmente on-chain. Il punto è che non si tratta di valute di banche centrali dell'Eurosistema, ma di valute emesse da aziende private.

La terza categoria include cripto-attività diverse da ART e EMT, ossia una categoria residuale comprendente token che non rientrano né nella classificazione giuridica di ART, né in quella di EMT. Data l'assenza di attività sottostante, questi token sono sovente indicati anche come "unbacked token". Il macro-insieme in questione include gli *utility token*, definiti espressamente da MiCA come cripto-attività destinate esclusivamente a fornire accesso a un bene o servizio offerto dai rispettivi emittenti,[9] nonché altre cripto-attività che, pur non essendo specificamente definiti dalla normativa, ricadono comunque nella categoria miscellanea dei token che non sono né ART né EMT. Quest'ultima categoria comprende i token nativi delle blockchain, i *governance token* (tipicamente emessi a livello di smart contract e utilizzati per esercitare diritti di voto in contesti decentralizzati) e i *meme coin* (token motivati dall'hype della comunità, generalmente privi di utilità funzionale).

Il Considerando 22 lima ulteriormente i contorni del perimetro catturato da MiCA e precisa che sono fuori dall'ambito di applicazione del regolamento i token che non hanno un emittente identificabile, il che lascia fuori dall'ambito di applicazione Bitcoin e in teoria anche i meme coin emessi da ignoti.

Su queste basi classificatorie, MiCA istituisce un quadro regolatorio stratificato, indirizzato a emittenti, offerenti o soggetti che chiedono l'ammissione alla negoziazione, nonché ai CASP.

3 Emittenti di Token, Offerenti e Soggetti che Chiedono l'Ammissione alla Negoziazione

Partendo dalla classificazione dei token sopra descritta e derivando più di una influenza dal quadro della *Prospectus Regulation*, che già disciplina l'offerta pubblica e l'ammissione alla negoziazione di strumenti finanziari, MiCA disciplina diverse categorie di attori, quali emittenti, offerenti e soggetti che richiedono l'ammissione a una piattaforma di negoziazione autorizzata (i servizi specifici autorizzati ai sensi di

[7] Definizione giuridica contenuta nell'Art. 3.1(6) del MiCA.
[8] Definizione giuridica contenuta nell'Art. 3.1(7) del MiCA.
[9] Definizione giuridica contenuta nell'Art. 3.1(9) del MiCA.

MiCA saranno esaminati nella sottosezione successiva). Considerati i diversi rischi posti da ciascuna categoria di cripto-attività, MiCA contempla approcci regolatori distinti e talune esenzioni.

In primo luogo, va precisato che, indipendentemente dalla categoria di cripto-attività, le vendite private restano al di fuori del campo di applicazione del regolamento. Ciò include, ad esempio, investimenti in token regolati da accordi privatamente negoziati. Questo vale anche per gli accordi privati di pre-vendita di token, ampiamente utilizzati nell'industria per finanziare startup nelle fasi iniziali di un progetto. In pratica, dove non c'è sollecitazione pubblica dei risparmiatori MiCA non entra in gioco. Quando invece viene effettuata un'offerta pubblica (nel gergo di settore, una *initial coin offering*) oppure ha luogo un'ammissione alla negoziazione su una piattaforma di negoziazione autorizzata in UE (quello che in gergo si chiama *listing* presso un *exchange*), MiCA entra in gioco.

Il Titolo II di MiCA riguarda l'offerta al pubblico e l'ammissione alla negoziazione di cripto-attività diversi da ART e EMT. Per queste classi di asset, il regolamento adotta un approccio "light-touch", che non richiede un'autorizzazione preventiva scritta da parte dell'autorità nazionale competente (ACN). È tuttavia richiesto che venga redatto e notificato all'ACN un white paper conforme a MiCA,[10] distinto dai white paper commerciali tradizionali utilizzati per descrivere progetti tecnologici da una prospettiva di visione e utilità del prodotto. Questo documento rappresenta uno strumento di disclosure regolatoria, concettualmente analogo a un prospetto finanziario, ma più leggero, e deve includere dettagli di trasparenza, avvertenze per gli investitori e conformità a specifici requisiti formali, inclusi quelli relativi al formato elettronico.

Sebbene il Titolo II non comporti né autorizzazioni, né supervisione continua degli attori, le ACN conservano il potere di sospendere o vietare un'offerta pubblica o l'ammissione alla negoziazione in caso di white paper mancante o non conforme. L'obbligo di notifica di un white paper MiCA ai sensi dell'Articolo 8 ricade sull'offerente del token in caso di offerta pubblica (regolata dall'Articolo 4) o sul soggetto che cerca l'ammissione alla negoziazione (regolato dall'Articolo 5).

È rilevante sottolineare che, ai sensi di MiCA, non conta se il token non garantito sia offerto al pubblico dall'emittente stesso, da un'altra entità del gruppo o persino da un CASP durante l'erogazione dei propri servizi: chiunque indirizzi l'offerta al pubblico deve notificare un white paper conforme a MiCA. Lo stesso vale per l'ammissione alla negoziazione di cripto-attività non garantiti, indipendentemente dal fatto che l'ammissione sia richiesta da un'entità collegata al progetto sottostante o sia iniziativa di un CASP. Questo approccio, a nostro avviso, è coerente con la logica basata sul rischio, poiché mira al soggetto che genera il rischio portando sul mercato un dato token e innescando la sollecitazione pubblica degli investitori. In questo senso, è corretto affermare che il Titolo II.

[10] La disciplina è contenuta nel Titolo II in generale e più nel particolare negli Art. 4-6, 8-9.

Un approccio regolatorio significativamente più rigoroso è applicato agli stablecoin, riflettendo la complessità dei modelli di business sottostanti e i rischi specifici che i legislatori dell'UE intendono mitigare.

MiCA pone particolare enfasi sul mantenimento di riserve altamente liquide e adeguatamente sovracollateralizzate, al fine di ridurre i rischi di de-pegging, salvaguardare i diritti di rimborso dei detentori di token e contenere possibili scenari di "corsa agli sportelli". Per consentire una supervisione efficace di tali aspetti, MiCA si rivolge direttamente agli emittenti di stablecoin, richiedendo che siano soggetti finanziari autorizzati e vigilati, stabiliti nell'Unione.

Più nello specifico, per ART, regolati dal Titolo III di MiCA, l'emissione è limitata a soggetti autorizzati come emittenti ART ai sensi del Titolo III o già operanti con licenza di istituto di credito (banche), in ogni caso debitamente stabiliti e autorizzati in uno Stato membro. Pur potendo una persona diversa dall'emittente offrire ART al pubblico o chiedere la loro ammissione alla negoziazione, ciò non pregiudica i requisiti normativi dell'emittente ed è subordinato al consenso scritto preventivo dell'emittente stesso. Limitare l'emissione di ART a soggetti autorizzati e vigilati riflette il fatto che l'intero ciclo di vita di un ART — comprese riserve di *backing* e meccanismi di rimborso — è intrinsecamente collegato alle operazioni dell'emittente. L'UE ha quindi scelto di regolare direttamente l'emittente, sottoponendolo a supervisione prudenziale continua come soggetto finanziario regolamentato, comprendente il controllo del profilo aziendale e operativo, della governance e della gestione, delle politiche di investimento delle riserve, del personale e delle infrastrutture tecnologiche. A tal ultimo proposito, gli emittenti di ART sono inclusi tra le entità soggette altresì all'applicazione di DORA, il Regolamento europeo sulla cybersicurezza.

Un quadro regolatorio analogo si applica agli emittenti di EMT, sebbene soggetto a ulteriori restrizioni. MiCA non introduce un'autorizzazione dedicata per l'emissione di EMT, stabilendo piuttosto che solo soggetti già autorizzati nell'Unione come istituti di credito o IMEL possono offrire EMT al pubblico o richiederne l'ammissione alla negoziazione. Questo in un certo senso semplifica l'accesso al mercato a quegli attori già minuti di licenze bancarie o di licenze da IMEL, per altri versi richiede ai nuovi attori di mercato di passare per un regime autorizzatorio non originariamente pensato per le specificità dell'industria cripto. Come per gli ART, un soggetto diverso dall'emittente può offrire EMT al pubblico o cercarne l'ammissione, senza pregiudicare i requisiti dell'emittente e previo consenso scritto dello stesso.

Tali interventi pervasivi hanno il potenziale di sfrondare il mercato UE dagli attori meno dediti alla *compliance*, favorendo invece quelli più attenti e disposti a compromettere con la legge. L'impatto iniziale è già visibile, con noti operatori del settore costretti a uscire dal mercato UE per non conformità, con conseguente *de-listing* dei relativi stablecoin dalle piattaforme di negoziazione europee. Nel settore ART, l'esclusione più rilevante riguarda Pax Gold (PAXG), stablecoin ancorata all'oro, attualmente senza emittente autorizzato in UE ai sensi di MiCA. Per quanto riguarda gli EMT, l'assenza più significativa è quella di Tether, il cui USDT, lo

stabelcoin attualmente più diffuso al mondo, resta per il momento al di fuori del mercato regolamentato UE.

Questo approccio rigoroso all'emissione privata di stablecoin si sviluppa parallelamente all'esplorazione, da parte dell'Unione, di una *central bank digital currency* (CBDC), che esula dal campo di applicazione di MiCA e segue una logica istituzionale e giuridica completamente diversa.[11] Mentre MiCA mira a regolamentare i sostituti monetari emessi privatamente tramite supervisione prudenziale, le iniziative sulle CBDC riflettono la centralità persistente della sovranità monetaria pubblica.

4 Il Regime Autorizzatorio secondo il Regolamento MiCA

Come anticipato, MiCA introduce requisiti di autorizzazione per i soggetti che forniscono servizi relativi alle cripto-attività. A tal fine, la quinta direttiva AML aveva già definito due categorie di base di fornitori di servizi: i servizi di exchange tra valute virtuali e valute fiat e i *custodian wallet provider*. Ai fini di MiCA, tali categorie vengono riviste e integrate con nuove categorie ispirate alla regolamentazione finanziaria tradizionale, in particolare alla MiFID II.

Più nello specifico, MiCA stabilisce requisiti di autorizzazione per dieci distinti servizi per cripto-attività, tutti caratterizzati dal fatto di essere rivolti al cliente. Di conseguenza, alcuni operatori di mercato, come i *market maker*, ricadono al di fuori del perimetro di MiCA poiché non intrattengono relazioni dirette con la clientela.

A) Custodia e amministrazione di cripto-attività per conto di clienti. I servizi soggetti ad autorizzazione iniziano con la custodia e amministrazione di cripto-attività per conto dei clienti, definita come la conservazione o il controllo, per conto dei clienti, di cripto-attività o dei mezzi di accesso a tali cripto-attività, ove applicabile sotto forma di chiavi crittografiche private. Tale definizione è deliberatamente più ampia rispetto a quella del mero *custodian wallet provider* e corrisponde all'equivalente del servizio accessorio previsto nella Sezione B, punto (1), dell'Allegato I di MiFID II.

B) Gestione di una piattaforma di negoziazione. MiCA contempla poi la gestione di una piattaforma di negoziazione per cripto-attività, definita come la gestione di uno o più sistemi multilaterali che raccolgono, o facilitano la raccolta di, interessi di acquisto e vendita di terzi su cripto-attività, secondo le regole del sistema, in modo da dar luogo a un contratto, sia mediante scambio di cripto-attività per fondi, sia mediante scambio di cripto-attività per altri cripto-attività. Il legislatore europeo considera questo servizio equivalente alla gestione di un *Multilateral Trading Facility*

[11] Si vedano la 'Council proposal COM/2023/364 final' (2023), la 'Council proposal COM/2023/368 final' (2023) e la 'Council proposal COM/2023/369 final' (2023), unitamente indicate come *Single Currency Package*. Maggiori informazioni disponibili sul portale istituzionale: https://finance.ec.europa.eu/publications/ digital-euro-package_en.

(MTF) o di un *Organised Trading Facility* (OTF) ai sensi della Sezione A, punti (8) e (9), dell'Allegato I di MiFID II. In altre parole, si tratta di un vero e proprio mercato multilaterale regolamentato.

C) Servizi di scambio. MiCA disciplina poi lo scambio di cripto-attività per fondi, inteso come la conclusione di contratti di acquisto o vendita di cripto-attività con i clienti utilizzando capitale proprio. L'Articolo 60(3)(c) chiarisce che esso corrisponde all'attività di *dealing on own account* prevista nella Sezione A, punto (3), dell'Allegato I di MiFID II. In tali casi il fornitore internalizza l'ordine e realizza la conversione con il proprio capitale, agendo quindi come controparte diretta e non come agente del cliente.

Un servizio analogo, ma distinto, riguarda lo scambio di cripto-attività per altri cripto-attività, che segue lo stesso meccanismo, eccetto che la conversione avviene tra cripto-attività, implicando che il fornitore debba detenere una riserva propria di cripto-attività per eseguire il servizio. In entrambe le ipotesi, l'inoltro di un ordine di scambio a un terzo non costituisce servizio di scambio, ma un'attività diversa che richiede invece la licenza per ricezione e trasmissione di ordini (RTO), come dettagliato di seguito.

D) Esecuzione di ordini. MiCA regola anche l'esecuzione di ordini per cripto-attività per conto dei clienti, definita come la conclusione, per conto dei clienti, di accordi di acquisto, vendita o sottoscrizione di uno o più cripto-attività, inclusa la conclusione di contratti di vendita di cripto-attività al momento dell'offerta pubblica o dell'ammissione alla negoziazione. Si tratta di un vero e proprio servizio di brokeraggio, in cui il CASP agisce come agente, equivalente all'esecuzione di ordini per conto dei clienti prevista nella Sezione A, punto (2), dell'Allegato I di MiFID II.

E) Collocamento. Il collocamento di cripto-attività, definito come la commercializzazione di cripto-attività verso acquirenti per conto dell'offerente o di un soggetto ad esso collegato, costituisce un'altra categoria derivata da MiFID. Questa categoria mira a catturare intermediari che agiscono come sottoscrittori o collocatori di cripto-attività, sia sulla base di un impegno a sottoscrivere direttamente gli asset (sopportando quindi il rischio di invenduto) che senza, come previsto nella Sezione A, punti (6) e (7), dell'Allegato I di MiFID II, che MiCA richiama. La definizione è sufficientemente ampia da includere fornitori che offrono il servizio tramite piattaforme digitali, come dimostra il caso del Decubate launchpad, che ha ottenuto tale licenza nei Paesi Bassi.

F) Ricezione e trasmissione di ordini. MiCA regola ancora la ricezione e trasmissione di ordini (RTO) per cripto-attività per conto dei clienti, definita come la ricezione di un ordine di acquisto, vendita o sottoscrizione di uno o più cripto-attività da una persona e la trasmissione di tale ordine a terzi per l'esecuzione. Questa attività e

l'autorizzazione corrispondente riguardano qualunque instradamento di ordini in cui il CASP non internalizza l'esecuzione, agendo invece come agente, corrispondendo al servizio indicato nella Sezione A, punto (1), dell'Allegato I di MiFID II.

G) Consulenza. La fornitura di consulenza su cripto-attività, definita come l'offerta, l'erogazione o l'accordo di fornire raccomandazioni personalizzate a un cliente, su sua richiesta o su iniziativa del fornitore, riguardanti transazioni o l'utilizzo di servizi su cripto-attività, è trattata come equivalente alla *investment advice* prevista nella Sezione A, punto (5), dell'Allegato I di MiFID II.

H) Gestione di portafogli. Ancora, MiCa si cattura anche la gestione di portafogli, definita come la gestione di portafogli in via discrezionale su base cliente per cliente, comprendenti uno o più cripto-attività, è allineata al servizio di *portfolio management* previsto nella Sezione A, punto (4), dell'Allegato I di MiFID II. Questo servizio non andrebbe confuso con la mera consulenza. Chi riceve consulenza può far proprie o meno le raccomandazioni consulenziali, ma alla fine è il decisore e implementatore ultimo della propria strategia di investimento. Nella gestione di portafogli il prestatore del servizio effettua discrezionalmente le scelte di investimento, disinvestimento e reinvestimento eventuale.

H) Trasferimento di cripto-attività. Infine, MiCA disciplina la fornitura di servizi di trasferimento di cripto-attività per conto dei clienti, definita come il trasferimento, per conto di una persona fisica o giuridica, di cripto-attività da un indirizzo o account su registro distribuito a un altro. Il servizio ricorda da vicino i servizi di pagamento regolamentati ai sensi della PSD2, e ciò è confermato dal fatto che gli EMT sono considerati moneta elettronica secondo la Direttiva 2009/110/CE, il cui trasferimento richiede autorizzazione secondo PSD2. Ciò ha sollevato la questione se i CASP che prestano il servizio di trasferimento anche per EMT debbano essere autorizzati anche ai sensi di PSD2. La risposta è affermativa e si è concretizzata tramite una *no-action letter* emessa nel giugno 2025 dall'European Banking Authority (EBA), che ha qualificato tali servizi di trasferimento come servizi di pagamento secondo PSD2 quando hanno ad oggetto anche EMT [1]. Una conseguenza di tale interpretazione è l'introduzione di una doppia autorizzazione sotto MiCA e PSD2 per un servizio che, in sostanza, è unico. L'EBA stessa ha suggerito una riforma, consigliando alla Commissione UE, al Consiglio e al Parlamento di utilizzare il processo legislativo PSD3/PSR. EBA ha proposto o di rafforzare MiCA, tramite replicazione dei o rinvio incrociato ai requisiti PSD3/PSR pertinenti, oppure, in alternativa, modifiche mirate nel pacchetto legislativo PSD3, al fine di evitare la doppia autorizzazione per i CASP.

I) Servizi esenti da MiCA. Le attività di erogazione ed assunzione di prestiti (*lending* e *borrowing*) restano esplicitamente fuori dal perimetro di MiCA come

prevede il Considerando 94, così come lo *staking* in quanto tale, sebbene la custodia e amministrazione delle cripto-attività fornita contestualmente al servizio di *staking* sia regolamentata come sopra discusso.[12]

Anche il concetto più ampio di *decentralized finance* (DeFi) non rientra nell'ambito di MiCA. Tuttavia, qualora un servizio ricada in una delle dieci categorie regolamentate illustrate sopra, MiCA richiede che esso sia completamente decentralizzato, cioè fornito senza alcun intermediario, per rimanere fuori dal perimetro regolatorio, come stabilisce il Considerando 22. L'assenza di ulteriori criteri per determinare cosa costituisca un servizio "completamente decentralizzato" lascia incertezza significativa sul trattamento regolatorio di molti *decentralized exchange* (DEX). Ai fini del MiCA, non è sufficiente che una piattaforma di negoziazione si avvalga di *automated market maker* (AMM), elemento fondamentale dei DEX, per essere considerata fuori dall'ambito di MiCA. Infatti, la regolamentazione di secondo livello espressamente include gli AMM come uno dei possibili meccanismi di *trading* utilizzati da DEX non completamente decentralizzati e che ricondurre all'ambito applicativo di MiCA. Pertanto, le ACN devono valutare caso per caso cosa costituisca un servizio completamente decentralizzato fornito senza intermediari.

In conclusione, l'architettura regolatoria di MiCA dimostra una chiara preferenza per la regolamentazione degli attori di mercato identificabili e delle attività rivolte al cliente, lasciando in gran parte non esaminata come oggetto normativo l'infrastruttura tecnologica che abilita tali attività.

5 Il Progetto di Regolamento sulle Cripto-Attività nel Regno Unito

Conclusa la panoramica sul MiCA, questa sezione analizzerà il progetto di regolamento sulle cripto-attività in fase di lavorazione e adozione nel Regno Unito, per trarre progressivamente considerazioni comparatistiche rispetto al MiCA. Nell'aprile 2025, HM Treasury ha pubblicato un disegno di *Statutory Instrument* (SI) proponendo modifiche al *Financial Services and Markets Act* 2000 (FSMA) per includere l'industria dei cripto-attività nell'ambito della regolamentazione finanziaria del Regno Unito, principalmente mediante l'introduzione di nuove attività regolamentate. Una versione ampliata e aggiornata del disegno di SI è stata presentata al Parlamento il 15 dicembre 2025.

Il 16 dicembre 2025, la FCA ha pubblicato tre consultation papers — CP25/40, CP25/41 e CP25/42 — illustrando le regole dettagliate proposte e fornendo ulteriori indicazioni interpretative e applicative del SI. Ulteriori consultation paper

[12] Lo *staking* consiste nel bloccare cripto-attività in un protocollo proof-of-stake per partecipare alla validazione delle transazioni in cambio di una remunerazione. Diventa un servizio quando un CASP offre *staking* per conto di clienti, gestendo operativamente il processo di immobilizzazione e distribuzione dei *reward*.

sono arrivati e arriveranno nel corso del 2026. Non è chiaro come il processo di approvazione parlamentare del SI e delle regole FCA possa concludersi in tempo utile per lasciare margine alle aziende colpite di preparare le domande autorizzatorie e conformare le proprie caratteristiche operative alle norme in tempo per l'apertura del termine iniziale di presentazione delle domande, al momento previsto per un generico settembre 2026.

Venendo agli attori di mercato interessati dal progetto di regolamentazione, il SI introduce una singola macro-categoria denominata "*authorised cryptoasset firm*" (ACF), che ingloba i soggetti che nella terminologia del MiCA definiremmo CASP, sia gli emittenti di specifiche categorie di stablecoin (meglio discussi nel prosieguo).

6 Un'Analisi Comparata

Per quanto riguarda gli equivalenti britannici dei CASP, il progetto di regime britannico regola l'attività di custodia (*safeguarding*). Tale attività si estende non solo alle cripto-attività pure, ma anche alle cripto-attività legalmente qualificabili come investimenti specifici, ossia token che soddisfano i requisiti di titoli o strumenti contrattuali. Come spiegato nella documentazione a supporto del SI, i titoli e gli strumenti contrattuali rientrano già nel regime di custodia previsto per gli investimenti specifici; l'inclusione delle loro versioni tokenizzate nel perimetro del SI garantisce alla FCA la possibilità di affrontare i rischi specifici associati alle tecnologie digitali.

Il regime regolamentare disciplina inoltre gli operatori di piattaforme di negoziazione, categoria sostanzialmente corrispondente a quella omonima dal MiCA. Una questione chiave riguarda l'eventuale adozione di un approccio restrittivo simile a quello emergente nell'UE, dove, secondo l'European Securities and Markets Authority (ESMA), il libro ordini di una piattaforma di negoziazione autorizzata nell'UE dovrebbe essere separato da quelli di entità offshore appartenenti allo stesso gruppo societario. Al momento, la proposta contenuta nel Consultation Paper CP25/40 suggerisce un approccio britannico più flessibile: l'accesso a pool di liquidità globali appare consentito, a condizione che il rapporto con la clientela e la responsabilità regolatoria rimangano ancorati a un'entità giuridica del Regno Unito, con eventuali filiali estere che operano esclusivamente come infrastrutture funzionali e soggette a scrutinio caso per caso in sede di autorizzazione. I libri ordini che inglobano ordini da più paesi non sembrano quindi proibiti, ma neppure automaticamente consentiti.

Un'altra attività regolamentata è quella di *trading* in cripto-attività qualificati come *principal*, che sembra finalizzata a includere, tra gli altri, i desk di *principal dealing*, i *market maker* e i servizi di prestito di cripto-attività. In quest'area, l'UE e il Regno Unito potrebbero divergere significativamente. In base al MiCA, le uniche forme di *principal dealing* attualmente regolamentate riguardano i due servizi di scambio, sopra esaminati, dove il CASP esegue un ordine del cliente con capitale proprio. Di conseguenza, i market maker ricadono al di fuori dell'ambito di MiCA,

perché tipicamente questi soggetti non servono direttamente clienti, bensì si limitano ad assumere l'impegno di supportare la liquidità dei mercati multi-laterali. La categoria britannica sembra chiaramente mirata per coprire e regolare da subito più categorie di attori rispetto al MiCA.

L'attività di *trading* in cripto-attività qualificati come *agent* è definita in maniera ampia e sembra comprendere servizi sostanzialmente equivalenti all'esecuzione di ordini e alla ricezione e trasmissione di ordini (RTO) secondo MiCA.

L'attività di *arrangement* di operazioni in cripto-attività rappresenta un'ulteriore categoria estesa, destinata a includere, tra l'altro, le piattaforme di *lending* di cripto-attività. Ciò conferma ulteriormente che il prestito rientra pienamente nel perimetro delle proposte britanniche. Rispetto a MiCA, l'attività di *arranging* è sufficientemente ampia da comprendere funzioni analoghe al collocamento, incluse le piattaforme di lancio delle cripto-attività e gestione intermediate delle *initial coin offering*. Potrebbe inoltre catturare desk OTC che organizzano transazioni bilaterali o multilaterali di tali attività. Anche piattaforme peer-to-peer che hanno un intermediario potrebbero rientrare nel perimetro, nella misura in cui facilitano l'incontro tra domanda e offerta, sebbene la documentazione attuale non affronti esplicitamente questo punto.

Infine, le proposte britanniche introducono un'attività regolamentata dedicata allo *staking*, trattata separatamente dai *collective investment schemes*. Vi è un esplicito riferimento allo *staking* liquido (*liquid staking*),[13] con la precisazione che l'emissione di token di *staking* liquido è coperta dall'attività di *trading* (*dealing*). Di conseguenza, le imprese coinvolte nello *staking* liquido potrebbero necessitare di autorizzazioni separate o aggiuntive.

Al contrario, MiCA non regolamenta lo *staking* in sé, concentrandosi sulla custodia, che può essere accessoria alla fornitura di servizi di *staking* forniti direttamente dal custode. Ciò solleva una questione rilevante: il quadro britannico intende regolamentare lo *staking* solo quando ad esso si accompagna la custodia degli asset dei clienti o anche i modelli senza custodia? Il paragrafo 6.8 di CP25/40 tratta il caso di fornitori di servizi di *staking* che svolgono anche attività di custodia, suggerendo implicitamente che il punto è catturare anche gli operatori che forniscono lo *staking* senza custodia.

[13] Lo *staking* liquido è una variante del servizio di *staking* in cui il cliente, anziché immobilizzare direttamente le proprie cripto-attività, riceve in cambio un token rappresentativo della posizione (*liquid staking token*, LST), liberamente trasferibile e utilizzabile — ad esempio come collaterale in protocolli DeFi — pur continuando a maturare i *reward* di *staking*.

7 La Finanza Decentralizzata (DeFi): un Perimetro Regolatorio Incerto

La policy note pubblicata in aprile 2025, al paragrafo 2.10, specifica che il disegno di SI non include disposizioni specifiche per i modelli di finanza decentralizzata (DeFi). Quando le attività regolamentate sono svolte in maniera realmente decentralizzata, ossia in assenza di una persona identificabile che eserciti l'attività in modo professionale, i requisiti autorizzativi e regolamentari non si applicano. In tali casi, la FCA valuterà se vi sia una parte o più parti sufficientemente controllanti che dovrebbero invece essere soggette ad autorizzazione ai sensi della sezione 19 del *Financial Services and Markets Act* 2000 (il cosiddetto *general prohibition*).

Questo approccio è ribadito nel Consultation Paper CP25/40 (capitolo 6), dove la FCA riconosce esplicitamente che i modelli DeFi presentano gradi variabili di automazione e decentralizzazione e conferma di non voler adottare un approccio binario in termini di inclusione/esclusione dal perimetro regolatorio. Al contrario, le future linee guida si concentreranno su indicatori di controllo e (de)centralizzazione, sull'interazione tra DeFi e finanza centralizzata (CeFi) e sull'applicazione dei requisiti regolatori esistenti in questi contesti ibridi. Ulteriori indicazioni saranno inoltre fornite per chiarire come le imprese autorizzate ai sensi del FSMA dovranno mitigare i rischi di resilienza operativa e di criminalità finanziaria quando interagiscono con strutture altamente automatizzate o decentralizzate.

Rimane da vedere come questa intenzione si tradurrà in pratica, specialmente considerando che alcuni dei servizi di *borrowing* e *lending* più rilevanti operano attualmente attraverso protocolli DeFi.

8 Emittenti di Stablecoin: un'Analisi Comparata

Per quanto riguarda gli emittenti di stablecoin, il disegno di SI introduce la categoria delle "*qualifying stablecoins*", definite come stablecoin che si riferiscono a una o più valute fiat e mirano a mantenere un valore stabile detenendo tali valute fiat, o valute fiat unitamente ad altri asset, come riserve.

Per le fintech britanniche, una favorevole notizia è che, a differenza dell'UE, l'emissione di qualifying stablecoins non richiederà che l'emittente sia autorizzato come banca o istituto di moneta elettronica (EMI). Ciò detto, il regime presenta delle peculiarità che meritano approfondita analisi comparata.

In prima battuta si osserva che la definizione di qualifying stablecoin del SI non collima esattamente con quelle UE. Il raffronto definitorio indica che gli EMT ai sensi del MiCA sono compresi nel concetto di qualifying stablecoin, mentre sarebbero esclusi stablecoin il cui valore si riferisce a asset o diritti diversi da valute fiat, come le materie prime. Se tali token ricadessero al di fuori della definizione britannica di qualifying stablecoins, la loro emissione non costituirà un'attività regolamentata

di stablecoin secondo il disegno di SI e sarà invece trattata come cripto-attività generica.

Questa interpretazione è supportata dal regime di disclosure applicabile alle offerte pubbliche e alle richieste di ammissione alla negoziazione. Il SI richiede espressamente disclosure quando la cripto-attività qualificante mira o pretende di mantenere un valore stabile rispetto a un altro asset o diritto, includendo informazioni sulle caratteristiche finalizzate a mantenere la stabilità, sulla detenzione e gestione degli asset a supporto e sull'uso di algoritmi (articolo 13(1)(a) SI).

Ciò suggerisce che le cripto-attività con caratteristiche simili alle stablecoin, ma che ricadono al di fuori della definizione di qualifying stablecoins, saranno soggetti ad un processo di disclosure rafforzata piuttosto che ad un regime di autorizzazione dedicato.

9 Ambito territoriale della regolamentazione UK

Secondo il disegno di SI britannico, le imprese che operano direttamente o indirettamente con consumatori britannici dovranno ottenere l'autorizzazione nel Regno Unito, indipendentemente dal fatto che siano stabilite nel Regno Unito o all'estero. Ciò si applica all'operazione di piattaforme di negoziazione di cripto-attività qualificati, al *trading* di cripto-attività qualificati come *principal* o come *agent*, e all'*arranging* di operazioni in cripto-attività qualificati.

Al contrario, le imprese estere che svolgono le stesse attività esclusivamente per clienti istituzionali britannici non saranno tenute all'autorizzazione, purché tali clienti istituzionali non agiscano da intermediari tra l'impresa estera e i consumatori retail del Regno Unito.

Inoltre, le imprese necessiteranno di autorizzazione britannica se forniscono custodia di cripto-attività qualificati (e dei corrispondenti investimenti specifici) e attività di *staking* di cripto-attività qualificati, indipendentemente dal fatto che servano solo clienti istituzionali o anche consumatori retail. Una limitata eccezione si applica alle attività di custodia eseguite su indicazione di una persona già autorizzata a svolgere tale attività, modello più vicino al concetto di outsourcing regolamentato che a quello di fornitura indipendente.

Per gli emittenti di stablecoin il regime funzionerà invece in maniera in parte diversa, attraverso un test territoriale più sfumato. L'emissione è definita come comprendente tre componenti distinte: offerta, rimborso e mantenimento del valore della stablecoin qualificante. Svolgere anche una sola di queste attività da una sede nel Regno Unito è sufficiente a ricondurre l'impresa nel perimetro regolatorio britannico per l'emissione di stablecoin. Viceversa, qualora nessuna di queste attività sia condotta nel Regno Unito, l'autorizzazione non sarà richiesta, anche se la stablecoin è accessibile a utenti britannici.

Resta da capire come questo test territoriale si tradurrà in pratica, e in particolare occorre prestare attenzione a potenziali asimmetrie regolatorie rispetto al quadro UE.

I clienti britannici potrebbero essere esposti a tutele sostanzialmente diverse rispetto ai clienti UE tutelati dal MiCA. Questa divergenza diventerebbe ipoteticamente rilevante in scenari di *stress*, come una corsa agli sportelli su una stablecoin che interessa più giurisdizioni simultaneamente.

In forza del MiCA, gli emittenti di stablecoin autorizzati nell'UE sono soggetti a requisiti rigorosi sulla composizione delle riserve, sulla segregazione degli asset, sui diritti di rimborso e sui poteri di intervento della vigilanza, tutti volti a garantire che i detentori UE possano esercitare i propri diritti di rimborso anche in condizioni di mercato avverse. Al contrario, se una stablecoin è emessa al di fuori dell'UE e semplicemente offerta nel mercato britannico, i detentori del Regno Unito potrebbero non beneficiare di tutele equivalenti né dello stesso livello di supervisione o garanzia di rimborso, il che potrebbe fomentare corse agli sportelli di imprevedibile difficoltà gestoria, con potenziali conseguenze anche per i detentori UE.

10 Conclusioni Preliminari

L'impressione iniziale è che il quadro regolamentare britannico potrebbe risultare più permissivo per gli emittenti di stablecoin riferite a valute fiat, nonché per le stablecoin riferite ad altri asset o a panieri di asset. Al contrario, per la maggior parte delle altre attività connesse ai cripto-attività, le proposte britanniche riflettono un approccio ampio e "catch-all", che potrebbe porre sfide significative anche per le imprese già autorizzate secondo MiCA.

In termini pratici, tale divergenza implica che gli stessi servizi possano essere regolamentati in modi sostanzialmente differenti nel Regno Unito e nell'UE. Gli operatori su scala transfrontaliera potrebbero pertanto dover ripensare la *compliance* rispetto all'erogazione dei propri servizi. Tali scelte non sono meri dettagli giuridici, ma possono avere alcune importanti implicazioni concrete sulla liquidità, nonché sulla determinazione dei prezzi rispetto ai mercati in esame.

Inoltre, è chiaro che l'onere regolatorio per le imprese che intendono offrire dei servizi a clienti stabiliti nel Regno Unito potrebbe risultare più oneroso rispetto al presente. Ciò è particolarmente evidente in ambiti come, per esempio, *lending*, *borrowing* e *staking*, che sarebbero disciplinati diversamente nel Regno Unito e trattati come attività regolate. Infine, l'intenzione dichiarata del Regno Unito di escludere dal perimetro regolatorio la DeFi andrà valutata in concreto rispetto agli scenari ibridi. La prassi operativa della vigilanza e le linee guida delle autorità regolatrici potrebbero giocare un ruolo centrale nel chiarire il quadro regolatorio e facilitare la *compliance* per gli operatori nel Regno Unito e nell'UE.

References

1. European Banking Authority. Opinion on the application of PSD2 to crypto-asset transfers. EBA Opinion, 2025.

Ringraziamenti

È un piacere presentare il sesto volume della serie De Cifris Koine. Ci auguriamo che **Bitcoin e Blockchain** possa diventare uno strumento di riferimento per la comprensione critica di queste nuove tecnologie.

Ringraziamo chiunque abbia contribuito alla realizzazione del presente volume. Autrici ed autori per la loro attenzione ai dettagli e la loro costanza. Volontarie e volontari per il loro sempre presente impegno; senza di cui né questa collana né l'associazione potrebbero esistere. Vorremmo ringraziare in particolare: