Blockchain, Web3 and Cryptocurrencies

Blockchain, Web3 and Cryptocurrencies:

An Exploration of Freedom through Technology

By

Mongetro Goint

Cambridge Scholars Publishing

Blockchain, Web3 and Cryptocurrencies:
An Exploration of Freedom through Technology

By Mongetro Goint

This book first published 2026

Cambridge Scholars Publishing

Lady Stephenson Library, Newcastle upon Tyne, NE6 2PA, UK

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

Copyright © 2026 by Mongetro Goint

All rights for this book reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the copyright owner.

ISBN: 978-1-0364-7459-1
ISBN (Ebook): 978-1-0364-7460-7

Disclaimer

The information contained in this book is provided for educational and informational purposes only. It does not constitute investment, financial, tax, or other regulated advice or recommendations.

Blockchain and cryptocurrencies are constantly evolving technologies. Their legal, economic, and technical framework can change rapidly. Before making any decision, particularly one involving digital assets, it is essential to conduct your own thorough research and, if necessary, consult a qualified professional, such as a financial or legal advisor.

The author and publisher accept no responsibility for any consequences arising from the improper use of the information contained in this book.

TABLE OF CONTENTS

LIST OF FIGURES

PREFACE

Over the past fifteen years, blockchain has evolved from technological curiosity to the beating heart of a global digital transformation. When Bitcoin first appeared in 2008, few imagined that this innovation, born from the convergence of cryptography, decentralized economics, and network theory, had the potential to revolutionize the way we exchange, collaborate, and produce value through secure automation. Today, blockchains are used in sectors as diverse as finance, logistics, energy, artistic creation, and organizational governance. They have given rise to new economic models, new communities, but also new questions.

The aim of this book is simple: to give readers the keys to understanding a technology that, beneath its apparent complexity, addresses some very profound issues—trust, transparency, digital sovereignty, decentralization of power, traceability, and the resilience of information systems. While it is true that terms such as "blockchain," "cryptocurrency," "Web3," and "smart contract" have invaded the media, their meaning is often diluted between techno-messianic myths, financial opportunity discourse, and fears that are difficult to substantiate. It became necessary to get back to basics: to explain, contextualize, and make it intelligible.

This book offers an educational journey combining history, technology, sociology, and foresight. It begins with the scientific and philosophical foundations that make blockchains possible: asymmetric cryptography, game theory, distributed consensus, and decentralized governance. It then shows how cryptocurrencies have emerged as new vehicles of exchange, while detailing the limitations and controversies that accompany them: volatility, energy consumption, institutional adoption, and regulation. The

goal is not to convince or convert, but to clearly explain the mechanisms at work so that readers can form their own opinions.

Beyond digital currency, the book reminds us that blockchains have a much broader ambition: that of a decentralized web, often referred to as Web3. In this vision, individuals would no longer be mere users, but true actors owning their data, digital identities, and means of coordination. Current platforms—centralized, opaque, and dependent on business models based on data capture—could give way to distributed systems where trust comes from code rather than corporations. This does not mean the disappearance of intermediaries, but their transformation: from exclusive arbiters, they would become transparent facilitators.

However, the history of technology teaches us that nothing ever evolves in isolation. And it is perhaps in the convergence between artificial intelligence and blockchains that the most fascinating—and most strategic—horizon is emerging. AI, which is currently experiencing explosive growth, relies on massive access to data, increasingly sophisticated models, and colossal computing power. These elements raise critical issues: how can we guarantee the provenance and integrity of data? How can we make learning and decision-making processes transparent? How can we distribute the governance of AI systems to avoid unprecedented concentrations of power? How can we ensure the ethical sustainability of their uses?

Blockchains can provide credible answers to several of these questions: (i) through the immutable traceability of the data used to train the models; (ii) through the distributed governance of complex systems; (iii) through incentive mechanisms that encourage the emergence of collaborative networks; (iv) through the possibility of creating decentralized markets for data and models, making the ecosystem more competitive and less dependent on a few tech giants.

Conversely, AI can itself optimize blockchains: predictive analysis of network behavior, automated fraud detection, improved consensus algorithms, intelligent automation of smart contracts. We are probably only at the beginning of this symbiosis.

That is why it is now essential to renew our collective effort to understand these technologies, moving beyond sterile antagonisms. Blockchains are neither a panacea nor a threat, but a powerful set of tools just waiting to be explored, criticized, regulated, and used wisely. The question is no longer whether these technologies will matter, but how we choose to make them matter: in the service of a more inclusive, transparent, and resilient digital world—or, on the contrary, for the benefit of new technological monopolies.

This book offers readers the opportunity to address these questions with rigor and clarity. It is not a manifesto, much less a prediction. It is an invitation: an invitation to approach complexity with curiosity, to understand the mechanisms of a technology that already shapes our world, and to imagine the future we want to build with it.

Prof. Cyrille Bertelle
Université Le Havre Normandie

LIST OF ACRONYMS

2FA Two-Factor Authentication. 117

AI Artificial intelligence. 211

BTC bitcoin. 15, 30, 121, 190

DAO Decentralized Autonomous Organization. 187, 204, 248

DeFi Decentralized Finance. 152

DID Decentralized Identifiers. 194

EVM Ethereum Virtual Machine. 144

GAI Generative Artificial Intelligence. 216

IPFS InterPlanetary File System. 233

LLM Large Language Model. 216

NFT Non-Fungible Token. 102, 191

NLP Natural Language Processing. 214

PoS Proof of Stake. 36, 54, 62, 63, 251

PoW Proof of Work. 34, 36, 54, 55, 61, 98, 99, 250

SSI Self-Sovereign Identity. 185, 186, 194, 195

ZKP Zero-Knowledge Proofs. 160, 194

INTRODUCTION

For centuries, innovations have shaped human progress. The industrial revolutions of the 19th century marked a turning point with the invention of the steam engine, the telephone, the light bulb, and many other tools. These discoveries transformed societies, accelerating trade and redefining work. Mechanization enabled mass production, reducing costs and opening up international markets. Infrastructure developed at a rapid pace, connecting cities, nations, and then continents. This period of industrialization not only accelerated trade but also laid the foundations for globalized capitalism, where information and goods circulate with unprecedented fluidity.

However, it was truly in the 20th century that technological progress brought about a profound revolution in our daily lives. The emergence of computers, the Internet, and then the Web not only changed the way we communicate and work, but also transformed our very conceptions of value, exchange, and time. The Internet has established itself as the foundation of the digital economy, enabling the rise of dematerialized transactions on a global scale. Information now flows at the speed of light, abolishing distances and transforming economic and social relationships. Financial exchanges, communications, trade, and even access to knowledge are now governed by a continuous flow of data.

However, this massive centralization of information and value raises new questions: how can data confidentiality be preserved and how can we prevent digital power from becoming concentrated in the hands of a few players? While the internet democratized access to information, it also strengthened the control of a few entities over data. Through their control over digital infrastructure, GAFAM (Google, Apple, Facebook, Amazon, Microsoft)

largely dictate access to information, personal data management, and global economic flows, imposing the rules of the digital ecosystem.

A similar dynamic can now be observed with the rise of generative artificial intelligence. The major providers of artificial intelligence models (OpenAI, Google DeepMind, DeepSeek, Anthropic, xAI, Mistral, etc.) rely on centralized systems, fed by user interactions and data. These contributions, often involuntary, enrich proprietary algorithms, increasing the dependence of individuals and institutions on these platforms.

Thus, the internet and the web, once symbols of openness and decentralization, are tending to become a space dominated by a few entities capable of capturing and monetizing all information flows. Faced with this concentration of digital power, a new need is emerging: to establish trust without intermediaries, to give everyone back control of their data, and to reinvent the circulation of value on a global scale.

It is in this context that, in 2008, Bitcoin was born, driven by a radically different vision: to enable peer-to-peer exchanges of value without a central authority. This initiative is based on a revolutionary concept: blockchain. This technology makes it possible, for the first time, to transfer digital value securely, transparently, and without a centralized intermediary. In fact, to transfer bitcoins, the native digital asset of the Bitcoin network, no bank or institution is required, just a distributed network of participants who collectively validate transactions. This philosophical and technical breakthrough introduces a new form of trust, namely that placed in code and distributed consensus rather than in centralized authorities.

Blockchain, the technology behind Bitcoin, is more than just a ledger for managing financial transactions. It embodies a philosophy of decentralization. Unlike traditional systems that rely on trusted third parties, it guarantees data integrity through a distributed, transparent, and secure network. For example, a transfer of funds between two people located thousands of

miles apart can be made without going through a bank, in just a few minutes, with reduced fees and increased security. Since the emergence of Bitcoin, the scope of blockchain has expanded considerably, now touching on areas as diverse as finance, smart contracts, digital identity, and even supply chain management.

When I first discovered blockchain more than ten years ago, I was confused by the (apparent) complexity of this technology. The available resources were scattered and often not very educational. I then embarked on a quest for understanding, deepening my knowledge through extensive research, discussions with experts, and ultimately, obtaining a Ph.D. in the field. My journey led me to a simple realization: although many have heard of blockchain, few truly grasp its full potential.

This book was born out of this observation. Its goal is to share the knowledge I wish I had had when I started out—and much more. This book is not an encyclopedia, but a structured exploration, both theoretical and practical, of blockchain, Web3, and cryptocurrencies. It questions the potential of these technologies, not only on our economy, but also on our freedoms. Among these freedoms is the possibility of regaining control over our data, freeing ourselves from traditional intermediaries, and getting involved in more open, transparent, and decentralized systems.

Whether you are curious, knowledgeable, or a professional, this book offers a clear understanding of the challenges, opportunities, and limitations of this innovation. Understanding blockchain and its ecosystem may also mean understanding a new way of thinking about freedom in the digital age.

CHAPTER 1

DEFINITION AND HISTORY OF BLOCKCHAIN

Blockchain is often perceived as a recent technological innovation, but its fundamental concepts echo ancient practices. To fully understand this technology, it is interesting to look back at a unique, thousand-year-old monetary exchange system: that of the Rai stones of the Yap Islands.

Blockchain explained through the story of the Rai stones of the Yap Islands

To understand blockchain technology as a whole, it is crucial to return to its original purpose, which is the exchange of value. It is precisely for this reason that the first blockchain, Bitcoin, was created in 2008 and implemented in 2009, introducing the digital currency bitcoin. In order to start with an explanation of blockchain technology, I have chosen to go back to the history of one of the oldest monetary exchange systems, the "rai stones" of the Yap Islands (Fitzpatrick and McKeon, 2019, 7).

The exchange systems used by the Yapese and Bitcoin differ significantly. However, certain underlying concepts allow us to establish a link between them. These concepts include value accepted by the community, a decentralized transaction registry system, and trust in scarcity as the basis of value.

Rai stone blocks as a medium of exchange

Throughout human history, a wide variety of objects have been used as currency. By the 19th century, the inhabitants of the small Micronesian island of Yap used a rather unusual form of traditional currency called "rai stones." These were huge limestone discs, often quarried on the island of Palau, located hundreds of kilometers from Yap. The stones were then transported by canoe to the Yap Islands, a perilous journey. Once they arrived at their destination, they were used as a means of payment for goods and services. However, these stones could be several meters in diameter and weigh several tons, making them impossible to physically move. So, the transfer of ownership was simply done by informing the Yapese community of the change of ownership (Fitzpatrick and McKeon, 2019, 8-9).

In an era when written records did not yet exist, the community relied on collective memory to keep track of transactions. Each villager mentally recorded who owned each stone, from whom they had obtained it, and when the transaction had taken place. In the event of a dispute, the Yapese could consult other members of the community to verify the information. This system was one of the earliest known examples of a decentralized transaction ledger, where trust was distributed among members of the community (Fitzpatrick and McKeon, 2019, 10).

Limits of transactions using Rai Stones

The use of rai stones as a medium of exchange on the Yap Islands was both ingenious and fascinating. However, this system had inherent limitations. As exchanges multiplied and the number of participants grew, maintaining accurate mental records became increasingly difficult. The oral transmission of information carried significant risks: forgetfulness, communication errors, or even intentional manipulation. Trust, therefore,

relied entirely on the reputation of community members and their ability to accurately remember past transactions (Fitzpatrick and McKeon, 2019, 11).

Added to these cognitive and social constraints was another major practical drawback: the sheer weight of the stones themselves. Their size and mass made them impossible to move physically, which severely limited the fluidity of trade. Although perfectly suited to the cultural and geographical context of the Yapese, this monetary system was ultimately unable to evolve with the growing complexity of economic interactions.

Notaries as centralized trusted third parties

With the evolution of societies and the increasing complexity of trade, oral or community registers, such as those of the Yapese, have shown their limitations. To meet this need for reliability and traceability, specialized institutions have been created to guarantee the authenticity of transactions. This is the role of the notary.

The office of the notary is not a modern invention. Its origins can be traced back to ancient Rome, where public officials called *scribae* (scribes) were employed to record public proceedings, transcribe state papers, and register the decrees and judgments of magistrates (Smith, 1875, 1012). Later, with the invention of shorthand, a new type of writer called a *notarius* emerged, originally a stenographer who took down statements in shorthand (Notary NI, 2016). Over time, the *notarius* became a registrar attached to high government officials, and the title eventually gave its name to the modern notary.

As Chaserant and his colleagues (Chaserant et al., 2021, 7) demonstrate, the notary acts as a centralized trusted third party, producing what they call "institutional trust" to secure exchanges. The notary's mission is to verify the identity of the parties, record transactions in an official register, and ensure their legal validity. When a piece of land or a house is sold, for example, it is

not only the verbal agreement between the buyer and the seller that confers legitimacy on the transaction, but above all the notarized deed recorded in the archives. The system is therefore based on a recognized authority that ensures a certain level of reliability in transactions.

However, this centralization also has its limitations. As the same authors note (Chaserant et al., 2021, 58), trust based on a single institution remains vulnerable: registers can be subject to human error, fraud, manipulation, deterioration, or loss in the event of a disaster. In addition, access to them may be restricted or subject to considerable delays, which reduces the fluidity of transactions.

According to the authors of an article on digital notarial policy, published in 2023 (Namont Dauchez et al., 2023, 47), blockchain technology does not eliminate the need for notaries but renews their utility. Thus, whether through the collective memory of the Yapese or the centralized authority of the notary, the fundamental need remains the same: to ensure a reliable registry that guarantees ownership and transactions. It is precisely this problem that blockchain provides an innovative solution to. It replaces the centralized trusted third party with a decentralized, transparent, and secure digital registry.

A decentralized digital transaction ledger

The examples of rai stones and notaries show that societies have always sought to secure trade and guarantee property ownership. Each approach has its strengths and limitations: collective memory relies on the vigilance and loyalty of participants, while centralized notaries depend on the integrity of a single authority, can be costly or slow, and expose the system to the potential loss, destruction, or alteration of the central register.

Blockchain represents a new stage in this evolution. It combines the advantages of the two previous systems while eliminating their main

disadvantages. It offers a distributed, secure, and tamper-proof ledger, where trust is no longer placed in a single person or institution, but in an entire network made up of multiple actors.

Instead of stones or notarized documents, blockchain records digital assets in the form of digital tokens and logs each transaction in a transparent and immutable manner. Each participant holds a complete copy of the ledger, while cryptographic mechanisms guarantee the authenticity and validity of exchanges without the need for a central intermediary.

Thus, blockchain draws on ancient principles (decentralization, trust in shared ledgers, transfer of value) and modernizes them through technology. By creating Bitcoin, Satoshi Nakamoto transformed these historical concepts into a digital system capable of responding to the economic and social challenges of the digital age.

Definitions of blockchain

The creator of the blockchain did not provide a formal definition in his white paper,[1] published in 2008 (Nakamoto, 2008). The term "blockchain" does not even appear explicitly in Bitcoin's founding document. Entitled "Bitcoin: A Peer-to-Peer Electronic Cash System," this text describes only the fundamental principles and mechanisms on which the system is based.

The word "blockchain" became popular after the practical implementation of the concept with the launch of Bitcoin in January 2009. The exact definition of blockchain continues to be the subject of intense debate, both in the scientific community and among researchers and enthusiasts of this emerging technology. Some try to formulate often abstract definitions, while

[1] **White paper**: an informative document, usually published by an organization or institution, which presents a problem, offers an analysis, and proposes solutions or recommendations.

others propose approaches that more closely reflect their personal vision or interests. As a result, there is still no unanimously accepted definition.

Considering the many facets (ideological, technical, and functional) surrounding blockchain, I propose two definitions in this book, which I hope will be convincing: a general definition, followed by a technical definition.

General definition

Blockchain is **an interactive, shared protocol that operates in a decentralized manner, i.e., without a central control entity, enabling transactions to be carried out and stored securely and transparently**.

Let's analyze each aspect of this general definition:

- **Interaction and sharing**: A blockchain network is considered interactive because participants work together to validate what is added to the ledger, i.e., transactions. It is shared because all participants see and keep an identical copy of this ledger.

- **Decentralization**: Blockchain operates in a decentralized manner, meaning that no central authority can unilaterally decide on the rules or operation of the network. This ideology is radically opposed to that of traditional systems, such as banking systems, which are subject to the authority of a central bank responsible for monetary policy. In a blockchain, the entire network collectively holds the power of control, based on rules, consensus mechanisms, and computer algorithms.

- **Security and transparency**: Blockchain guarantees transaction security through cryptography,[2] which is used to verify and validate

[2] **Cryptography**: discipline that studies mathematical techniques related to information security.

operations. All transactions are transparent and can be viewed by all network participants.

Technical definition

A blockchain is **a peer-to-peer distributed digital ledger, in which data is regularly grouped into blocks, verified and validated by consensus mechanisms, and secured by cryptography to be immutable and tamper-proof**.

Let's analyze each aspect of this technical definition.

- **Grouping data into blocks**: To better understand the term "blockchain," it is useful to break it down into two parts: 'Block' and "Chain." The word "block" refers to the way data is stored, i.e., grouped into consecutive sets in a distributed ledger. The word "chain" refers to the way these data blocks are linked together. Each block contains a cryptographic reference to the previous block, thus forming a secure and unalterable chain.

- **Operation using consensus mechanisms**: Data blocks in a blockchain are created, verified, and validated by the various participants before being added to the chain at regular intervals. Since a blockchain network is made up of a group of participants called nodes, which are involved in validating transactions and ensuring the security of the system, it is necessary to define an unambiguous way for them to agree on how the process should unfold. This role is fulfilled by consensus mechanisms, which are built into the blockchain's computer protocol. This ensures that every transaction recorded in the ledger has been collectively verified and validated, making it impossible to fraudulently introduce information.

- **Cryptography-based security**: Cryptography, which encompasses all mathematical and computer techniques related to information security, plays a central role in ensuring a high level of security in blockchain data management. It not only guarantees data confidentiality, but also ensures its integrity and authenticity.

- **A peer-to-peer distributed ledger**: Blockchain is based on a network of computers connected in peer-to-peer mode, where each node holds a complete copy of the ledger. Data blocks are thus replicated and shared directly between nodes, without going through a central server. This architecture prevents the concentration of information in the hands of a single entity and illustrates the truly distributed and decentralized nature of the blockchain protocol.

In the two definitions of blockchain that I have provided, I have referred to the concepts of distribution and decentralization, which are neither synonymous nor interchangeable. A system is said to be "distributed" when data is spread across multiple machines or nodes, whereas it is "decentralized" when control, authority, and decision-making power are themselves shared among multiple entities. I will discuss these two concepts in detail at the beginning of the second chapter.

History of blockchain technology

Originally created for the financial sector, blockchain technology now has a long history. The many innovations associated with it since its creation make it a remarkable advance, whose evolution to date is as impressive as it is promising. But where does blockchain really come from, and what were its original motivations?

Bitcoin, the origin of blockchain

The first blockchain was implemented in January 2009, with the creation of the digital currency bitcoin. The real identity of its creator remains unknown to this day. Only his pseudonym, "Satoshi Nakamoto," is known. It was under this name that he published the white paper describing his protocol on bitcoin.org in October 2008 (Nakamoto, 2008). He also publicly unveiled his work in a message posted on the metzdowd.com forum.[3] A veritable mythology has grown up around the figure of Satoshi Nakamoto—a subject we will discuss in detail at the end of this chapter.

Blockchain technology forms the underlying structure of Bitcoin, and the two are historically linked. However, it is important to emphasize that Bitcoin is not synonymous with blockchain, and vice versa. Indeed, many blockchains exist today, often very different from Bitcoin, both technically and in their use cases. This confusion stems in part from the fact that Bitcoin was the first concrete application of this technology. It is therefore common for the terms to be used interchangeably, when in fact they should be differentiated. Blockchain is the technology that powers the digital currency bitcoin, and Bitcoin was the first implementation of blockchain technology. To draw an analogy, blockchain is to Bitcoin what the Internet is to the Web.

Blockchain emerged in the context of a major economic crisis. First, there was the subprime mortgage crisis in the United States beginning in 2007, which quickly had global repercussions, followed by the financial crisis in late summer 2008, often considered the second phase of the 2007-2008 global crisis.[4] This crisis profoundly shook the global banking system, leading to an economic recession with serious social and political consequences.

[3] `https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html`. Accessed: September 13, 2023

[4] **2007-2008 financial crisis**: it is considered the greatest economic crisis of the 21st century.

Faced with growing mistrust of financial institutions, Nakamoto presented a novel payment system based on a disruptive approach in his October 2008 white paper (Nakamoto, 2008). He published the source code[5] for his protocol as open source software, meaning it was freely accessible, modifiable, and redistributable. The Bitcoin network was thus launched in January 2009.

Satoshi Nakamoto's central idea was to create a free digital payment system that would operate without a central control entity and enable peer-to-peer value exchanges.[6] This concept is explained in detail in the Bitcoin white paper. By analyzing the Bitcoin protocol and blockchain technology in general, we can see Nakamoto's libertarian political vision, which goes beyond the monetary framework to extend to the digital realm. For him, "Code Is Law", as Lawrence Lessig pointed out in his book, *Code: Version 2.0* (Lessig, 2006, chap. 1).

On the monetary front, Nakamoto rejects the idea that money is limited to a combination of physical objects (coins, banknotes, checks, etc.) or traditional electronic instruments. On the other hand, he questions the notion that currency must be controlled by centralized institutions, such as governments or central banks, and regulated by state laws. Thus, when Nakamoto's vision was realized in 2009, the first blockchain network (Bitcoin) was born, along with its digital asset of the same name. There is an important spelling distinction to note. "Bitcoin" with a capital "B" refers to the blockchain network created by Nakamoto, including the protocol as a whole. Meanwhile, "bitcoin," with a lowercase "b," (except at the beginning of a sentence) refers to the digital asset, the cryptocurrency used to operate

[5] `https://github.com/trottier/original-bitcoin/`. Accessed: September 13, 2023

[6] **Peer-to-peer exchange**: a model of exchange between two entities without an intermediary.

this network. The latter is the unit of account of the decentralized system. It is often abbreviated as BTC.

Before delving into the mystery surrounding the identity of Bitcoin's creator, it is worth questioning the very nature of the invention attributed to Satoshi Nakamoto: Can bitcoin truly be described as a currency? While its technical architecture is unanimously praised for its innovative, even disruptive, nature, its economic status remains controversial. The debate pits proponents of a new form of digital store of value, seen as an alternative to existing monetary systems, against defenders of traditional sovereign currencies, which guarantee macroeconomic stability and state sovereignty. These issues will be analyzed in depth in Chapter 4, which is devoted to cryptocurrencies and tokens. We will show why bitcoin is technically classified as a "cryptocurrency," before examining the decisive question of its functional reality: Does bitcoin, in practice, fulfill the classic economic functions of a currency? In the meantime, let's focus on the mystery surrounding the founding figure behind the Bitcoin protocol.

Who is Satoshi Nakamoto, the creator of Bitcoin, really?

To this day, the creator of Bitcoin (and blockchain technology) remains one of the most famous mysteries in the history of technology. The author name "Satoshi Nakamoto" is associated with the 2008 publication of the Bitcoin white paper (Nakamoto, 2008), a concise and detailed eight-page technical document describing how the protocol works. At the time of writing (December 2023), no convincing evidence has been put forward to reveal the true identity of Bitcoin's creator. Most people, finding it difficult to determine the real identity behind the mysterious figure of Satoshi, simply speculate. Some have even attempted to usurp his identity—we will return to this subject later.

To fully understand the context in which Bitcoin was introduced and the traces of its mythical creator, it is essential to delve into the world of the Cypherpunks. This is an informal group of individuals passionate about privacy and the security of information and communications, sharing a common vision of actively using cryptography to guarantee these rights. This movement was born in the 1990s, and the Cypherpunks manifesto was made public in 1993 (Hughes, 1993), while members of the movement exchanged ideas and opinions via the "Cypherpunks Mailing List".[7] Satoshi Nakamoto also sent an email[8] to this mailing list, which repeats his message introducing Bitcoin, posted on metzdowd.com.[9] He described how the protocol works and the motivations behind its creation.

If we trace Satoshi Nakamoto's digital footprints, we can see that his last publicly posted message before disappearing was on December 12, 2010. This message was posted on bitcointalk.org,[10] a discussion forum for Bitcoin technical development. In his message, he suggested changes to the protocol to developers. The history of all of Satoshi's discussions on this forum can be traced back. The creator of Bitcoin also used other channels of communication, such as email, to communicate with key players involved in the initial development of Bitcoin. However, the Bitcoin talk forum remains the main public platform where he shared his ideas and communicated with the community interested in his protocol.

[7] https://mailing-list-archive.cryptoanarchy.wiki/. Accessed: December 11, 2023

[8] https://www.bitcoin.com/satoshi-archive/emails/cryptography/1/. Accessed: December 11, 2023

[9] https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html. accessed: September 13, 2023

[10] https://bitcointalk.org/index.php?action=profile;u=3;sa=showPosts Accessed: December 12, 2023