TO ALL THE HATERS AND DENIERS

WHO SAY BITCOIN IS USELESS OR DANGEROUS

BITCOIN IS OUT THERE, EVERY DAY, EVERY HOUR, IN COLLAPSED ECONOMIES AND IN THE DARKEST CORNERS OF THE WORLD, HELPING PEOPLE THAT NO ONE ELSE IS WILLING TO HELP. BEING A LIFELINE FOR *ANYONE*

FIAT MONEY HAS FAILED MOST PEOPLE ON EARTH BADLY. OUR MONETARY AND "AID" SYSTEMS EXPLOIT AND REPRESS INSTEAD OF DELIVERING PROSPERITY AND FREEDOM

BUT BITCOIN IS SLOWLY, STEADILY, UNITING, ENRICHING AND LIBERATING THE WORLD

—ALEX GLADSTEIN

I dedicate this work to the Human Rights Foundation..

Table of Contents

- 1. Why Bitcoin Matters
  - 1.1 Introduction to Bitcoin Technology
  - 1.2 Attributes of the Bitcoin Network
  - 1.3 Bitcoin and Human Rights
  - 1.4 The Byzantine Generals Problem
  - 1.5 Bitcoin Whitepaper
  - 1.6 Academic Origins
- 2. Bitcoin and Cryptography
  - 2.1 Blockchain: Bitcoin's Ledger
  - 2.2 Consensus Rules
  - 2.3 Bitcoin Security Model
  - 2.4 Hash Functions
  - 2.5 Digital Keys
  - 2.6 Digital Signatures
  - 2.7 Receiving Addresses
  - 2.8 Wallets
- 3. Transactions
  - 3.1 Inputs, Outputs, UTXOs
  - 3.2 SegWit—Segregated Witness and Transaction Malleability
  - 3.3 MultiSig: Multi-Signature Transactions in Bitcoin
  - 3.4 Bitcoin Script
  - 3.5 Miniscript
  - 3.6 CoinJoin
  - 3.7 Block Explorers
  - 3.8 Transaction Fees
  - 3.9 Practice: My First On-Chain Bitcoin

- 4. P2P Network
  - 4.1 Bitcoin Nodes
  - 4.2 Mempool
  - 4.3 Mainnet
  - 4.4 Regtest
  - 4.5 Testnet
  - 4.6 Signet
  - 4.7 Forks
- 5. Mining
  - 5.1 Energy: Utilization and Infrastructure Development
  - 5.2 Proof-of-Work
  - 5.3 Timechain
  - 5.4 Controlled Supply
  - 5.5 Solo Mining and Bitcoin Resilience
  - 5.6 Pool Mining
  - 5.7 Mining Hardware
  - 5.8 51% Attack
  - 5.9 Stratum V2
- 6. Bitcoin Core
- 7. BIPS—Bitcoin Improvement Proposals
- 8. RPC API do Bitcoin Core
- 9. Lightning Network
  - 9.1 BOLTs—Basics of Lightning Technology
  - 9.2 Payment Channels
  - 9.3 Lightning Nodes
  - 9.4 Network Explorers
  - 9.5 Practice: My First Bitcoin on the Lightning Network
- 10. Freedom Technologies
  - 10.1 Cypherpunks
  - 10.2 JoinMarket e Jam
  - 10.3 E-cash—Federated Chaumian Mints
  - 10.4 Nostr
  - 10.5 Value4Value
  - 10.6 Democratization of Science
  - 10.7 The Bitcoin Dev Project
  - 10.8 Bitcoin Optech
- 11. Career in Free and Open Source Software Development
  - 11.1 Philosophy of Bitcoin Development
  - 11.2 Bitcoin FOSS Development
  - 11.3 Chaincode Labs
  - 11.4 Summer of Bitcoin
  - 11.5 Scalar School
- 12. Bitcoin is For Everyone
- 13. Powered By Bitcoin
- 14. Final Notes
  - 14.1 Disclaimer

– [14.2 Contact](

1. Why Bitcoin Matters

"A mysterious new technology emerges, seemingly out of nowhere, but actually the result of two decades of intense research and development by nearly anonymous researchers. Political idealists project visions of liberation and revolution onto it; establishment elites heap contempt and scorn on it. On the other hand, technologists – nerds – are transfixed by it. They see within it enormous potential and spend their nights and weekends tinkering with it. Eventually mainstream products, companies and industries emerge to commercialize it; its effects become profound; and later, many people wonder why its powerful promise wasn't more obvious from the start. What technology am I talking about? Personal computers in 1975, the Internet in 1993, and – I believe – Bitcoin in 2014."

—Marc Andreessen, Founder of Netscape, 2014

1.1 Introduction to Bitcoin Technology

One way to think of Bitcoin is as a sequence of atomic transactions. Each transaction is authenticated by a sender with the solution to a previous cryptographic puzzle that was stored as a script, using the Bitcoin Script programming language.

The new transaction is locked to the recipient with a new cryptographic puzzle that is also stored as a script, whose new owner possesses the solution to unlock future transfers.

Each transaction is recorded in the global public and immutable ledger, the blockchain. Only the owner of the private keys that generated the address where the bitcoins are located can unlock the value to be moved forward.

We use "Bitcoin" with an uppercase B when referring to the network, the system itself. "bitcoin" with a lowercase b refers to the currency, the values transferred through this system.

1.2 Attributes of the Bitcoin Network

- **Security**: The Bitcoin network is secure as long as more than 50% of participating nodes are honest.
- **Reliability**: The network state is maintained by all nodes, which distribute the ledger copy among themselves.
- **Decentralization**: All network nodes replicate transaction records, ensuring data distribution.
- **Peer-to-Peer Transactions**: Allows direct transactions between users without intermediaries or central authorities.

- **Accessibility**: Anyone can join or leave the network, validate transactions, or mine new coins at any time.
- **Transparency**: All transactions are publicly verifiable and available to all network operators.
- **Permissionless**: No credentials, identifications, or authorizations are required to participate in the network.
- **Globality**: The network operates without geographical restrictions and can be accessed from almost anywhere in the world.
- **Censorship Resistance**: There is no central authority that can prevent fund transfers between users.
- **Neutrality**: The network is indifferent to who, what, when, where, or why you are sending and receiving bitcoin.
- **Inelastic and Distributed Supply**: Bitcoin generation is self-regulated by mathematical algorithms and game theory models, ensuring a fair and predictable process.

1.3 Bitcoin and Human Rights

Despite short-term Bitcoin volatility and the need for digital literacy for full use, Bitcoin offers significant benefits for human rights and financial inclusion, especially where traditional alternatives are limited or ineffective. Here's why Bitcoin matters for human rights.

Alternative to the Current System

Most of humanity's dramas, such as endless wars, are due to money being manipulable, arbitrarily printed, and allocated for such purposes without the general population's consent. Bitcoin solves this with its transparent monetary policy and inelastic supply defined by the community at the code level.

Financial Inclusion for the Unbanked

Approximately 1.7 billion people worldwide lack access to traditional banking services. Bitcoin offers a viable alternative, requiring only internet access and a mobile device to participate in the financial network. In regions like Sub-Saharan Africa, where banking infrastructure is limited, Bitcoin usage is growing as a way to access financial services.

Financial Freedom and Protection from Oppressive Regimes

In some countries, authoritarian governments can freeze bank accounts or confiscate assets arbitrarily. Bitcoin offers a way to protect assets from these actions. In countries with political or financial instability, such as Venezuela, individuals use Bitcoin to safeguard their wealth from hyperinflation and government control.

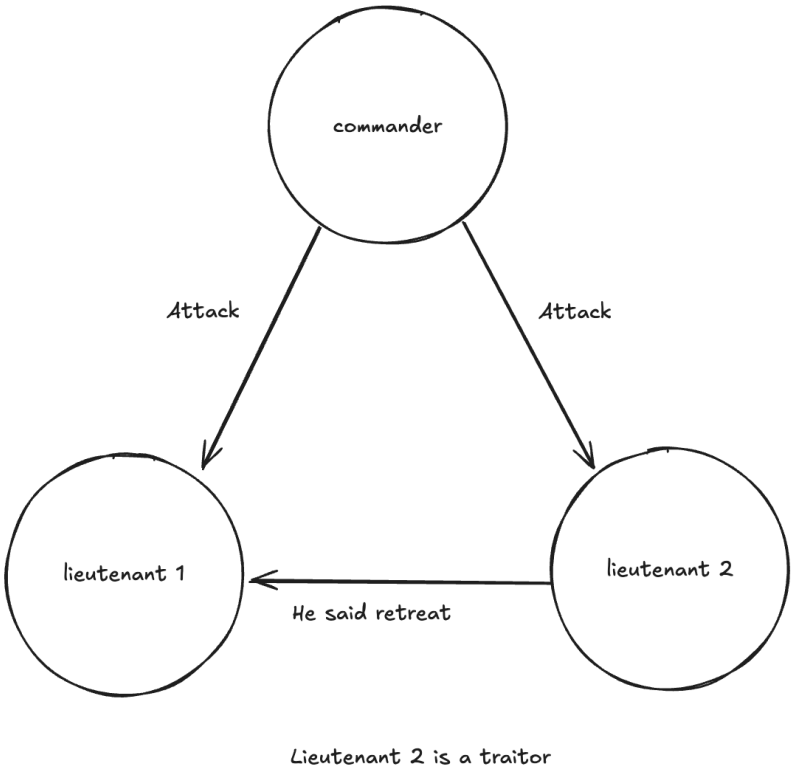

Figure 1: image1en

Facilitation of International Remittances with Lower Fees

Traditional money remittances, especially to developing countries, can have high fees and take days to process. Bitcoin allows near-instant transfers with much lower fees. Migrant workers sending money to their families can use Bitcoin to avoid high fees from services like Western Union, increasing the amount of money reaching the final recipients.

Personal Control Over Financial Resources

With Bitcoin, individuals have full control over their funds without needing intermediaries. This ensures greater autonomy and security in their financial transactions. In crisis situations, such as natural disasters or conflicts, where banks may be inaccessible, people can still access and use their funds with Bitcoin.

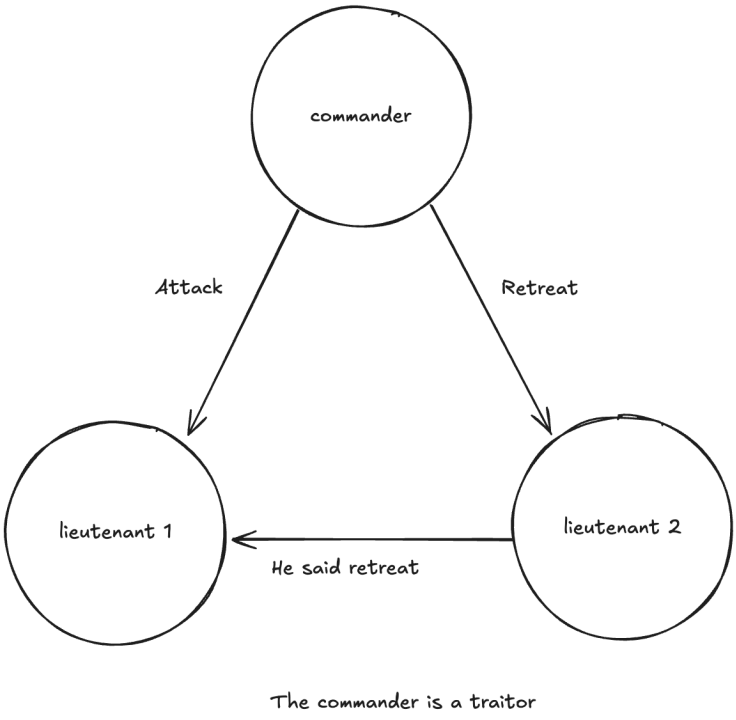

Figure 2: image2en

Transparency in Transactions and Fraud Prevention

The Bitcoin blockchain is an immutable public record of all transactions, reducing fraud possibilities and increasing transparency. Human rights organizations can use Bitcoin to receive donations transparently, allowing donors to see exactly how funds are used.

Incentive for Renewable Energy Use and Community Development

Bitcoin mining encourages the construction of electrical infrastructure in underdeveloped or hard-to-reach areas. The process has incentivized the use of renewable energy sources and innovation in energy efficiency, as miners seek cheaper and sustainable energy to maximize profits. Clean energy sources can enter negative pricing periods when production exceeds demand. In these moments, Bitcoin miners can use the excess energy to regulate grids, utilizing the energy and avoiding losses. Bitcoin mining can act as a flexible load, absorbing excess energy during production peaks and shutting down when demand increases.

Savings Method

Bitcoin is the best investment of all time and the best way to preserve purchasing power in the long term as fiat currencies are diluted by inflation. It is an extremely effective long-term savings tool as a scarce digital asset. Furthermore, most people do not have access to the stock market to preserve and grow their income.

Physical Money and Transaction Privacy are Disappearing

What happens when all our financial activity is trackable by a centralized entity, and we lose the financial privacy of physical money? What powers do governments and corporations gain when we trade our privacy and freedom for convenience? Each financial transaction reveals a vast amount of information about you, enabling control by corporations and governments, censorship of your transactions, and enabling surveillance and social engineering.

Bitcoin has been considered one of the main tools for guaranteeing human rights today. It is, in fact, a tool of freedom, especially useful in dictatorial countries with strict financial control of their citizens' bank accounts.

Bitcoin offers humans money that cannot be censored by authorities, cannot be devalued by governments, cannot be monopolized by corporations, cannot be easily mass-monitored, cannot be stopped by borders, and can be accessed by anyone. And that's why Bitcoin matters for human rights.

"Few people are looking at the intersection of monetary freedom and real freedom." —Alex Li, Bitcoin Development Lead, Human Rights Foundation

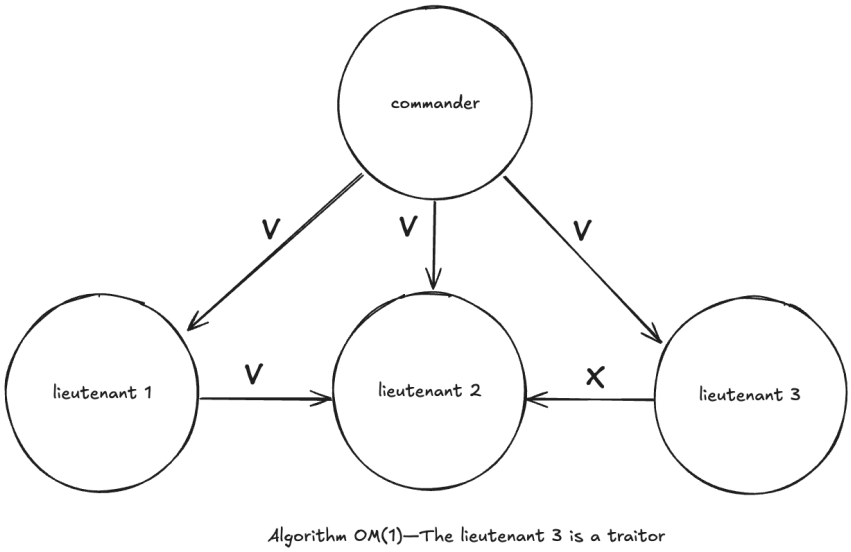

Figure 3: image3en

"Bitcoin is collaborative, decentralized, and aligns very well with the human rights movement." —Alex Gladstein, CSO, Human Rights Foundation

"Bitcoin is terrible for dictators." —Alex Gladstein, CSO, Human Rights Foundation

Recommended Reading: Check Your Financial Privilege.

1.4 The Byzantine Generals Problem

Bitcoin emerged as a solution created by Satoshi Nakamoto to address the Byzantine Generals Problem.

The Byzantine Generals Problem is a classic issue in computer science, specifically in the area of fault tolerance within distributed computing and distributed systems theory. It was first proposed by Marshall Pease, Robert Shostak, and Leslie Lamport in 1982, "expressed abstractly in terms of a group of Byzantine army generals camped with their troops around an enemy city."

In this scenario, a traitor (whether the Commander or a Lieutenant) prevents the group from reaching consensus. In a financial ledger, think of the traitor as a malicious party aiming to facilitate fraudulent transactions. As the number of parties in the system increases, the number of communication channels (and opportunities for distrust) increases exponentially. Imagine the complexity of building consensus with thousands or millions of parties involved. The following

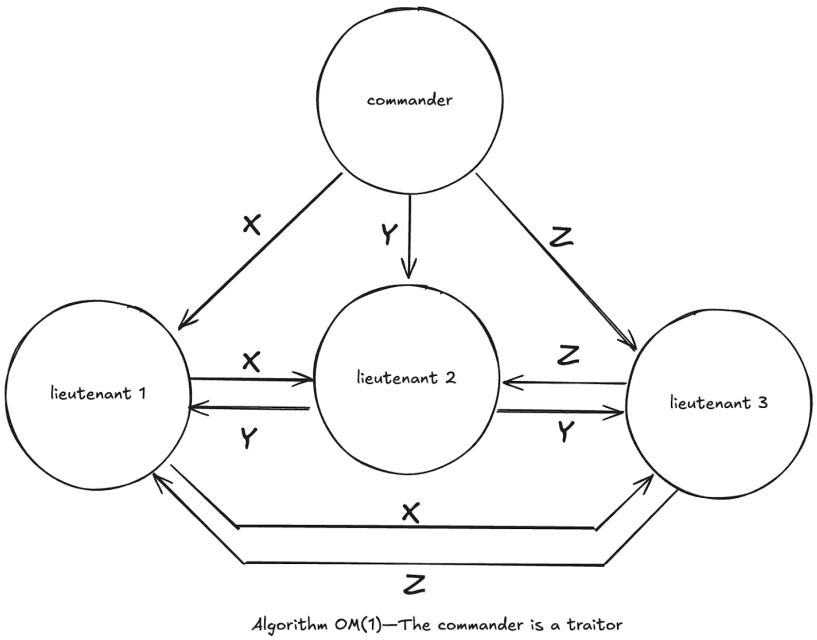

Figure 4: image4en

schemes are attributed to Lamport, Shostak, Pease, 1982.

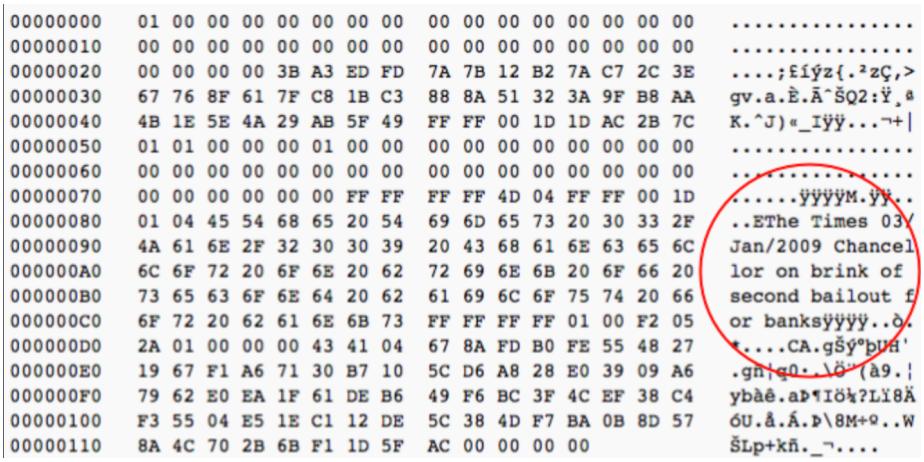

Figure 5: image5en

The solution to the Byzantine Generals Problem consists of combining probabilistic work (trial and error) in discovering the nonce that generates a hash equal to or below the difficulty level defined in the mining process, plus selecting the chain with the highest cumulative proof-of-work, meaning the greatest computational power employed to form it.

Bitcoin also solves the double-spending problem, ensuring that a digital asset (bits) cannot be duplicated or subject to copy-paste.

1.5 Bitcoin Whitepaper

Definição de Whitepaper

A whitepaper is an informative and technical document that presents the vision, methodology, and details of a project or technology, serving as a guide to understand its fundamentals and objectives.

The Bitcoin whitepaper, titled “Bitcoin: A Peer-to-Peer Electronic Cash System,” was released by Satoshi Nakamoto on October 31, 2008. It was published on a cryptography mailing list called “The Cryptography Mailing List” on the website metzdowd.com, detailing the structure and operation of a decentralized electronic payment system.

This document introduced innovative concepts that revolutionized the global financial system and have been used in various ways for the development of thousands of other cryptocurrencies and blockchain technologies.

It all started with Bitcoin, which remains the most important, decentralized, and robust candidate for a

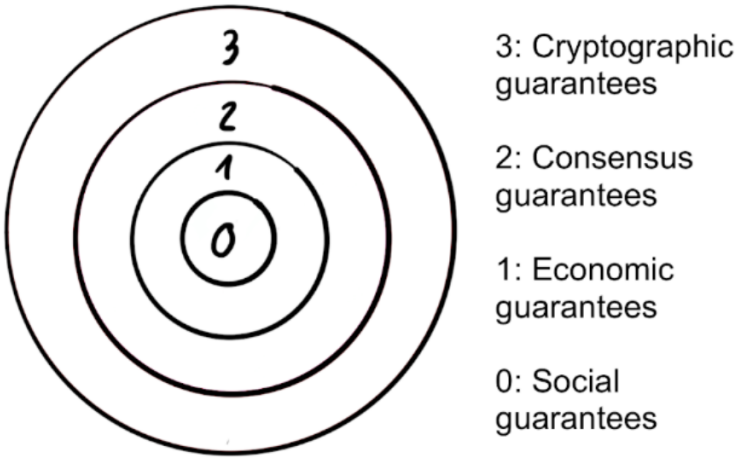

Figure 6: image6en