

"Pineapple and jalapenos is a  
good pizza topping"

Satoshi Nakamoto – Dec 10, 2010

From Seashells

to

Satoshis

From Seashells to Satoshis

In 'From Seashells to Satoshis,' A.J.R. Lewis explores the history of money, tracing its evolution to the revolutionary emergence of bitcoin. Discover how bitcoin is reshaping decentralization through sound money principles, art, physics, mathematics, and libertarian philosophy. This book reveals bitcoin's cutting-edge encryption techniques and previews the transformative impact on finance, technology, and personal liberty.

The physical-to-digital  
(r)evolution of money

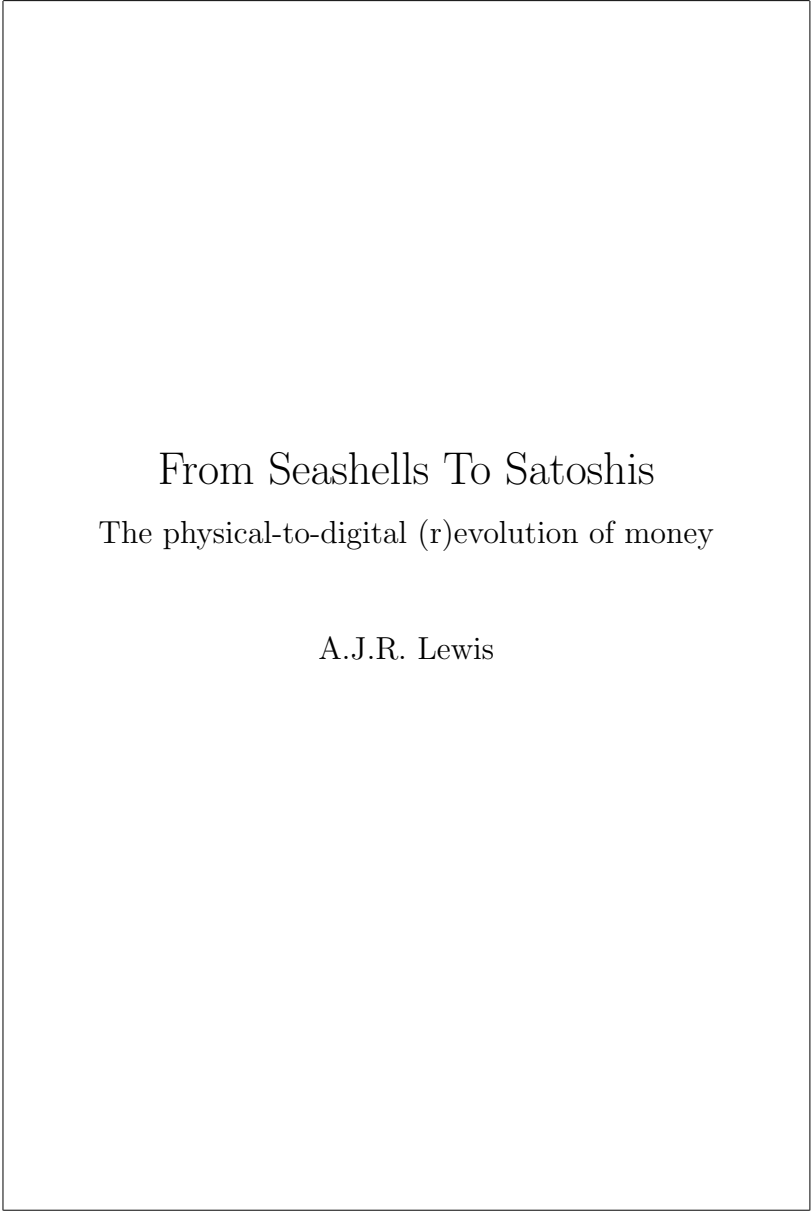
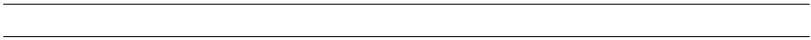


**Donate Bitcoin**

Send Bitcoin (BTC) to this  
deposit address.



Thanks for the support!



# From Seashells To Satoshi

The physical-to-digital (r)evolution of money

A.J.R. Lewis



**Copyright © 2024 A.J.R. Lewis**

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law.

For permission requests, write to the publisher, addressed “Attention: Permissions Coordinator”, at the address below.

A.J.R. Lewis  
London  
[hello@ajrlewis.com](mailto:hello@ajrlewis.com)

---

---

---

# Contents

<b>I</b>	<b>Genesis</b>	<b>1</b>
<b>1</b>	<b>Shelling Out</b>	<b>3</b>
1.1	Introduction . . . . .	4
1.2	Origin of Money . . . . .	5
1.3	So WTF is Money? . . . . .	6
1.4	So, Again, WTF is Money? . . . . .	7
1.5	Bitcoin Bookshelf . . . . .	11
1.6	What is Scarcity? . . . . .	11
1.7	section name . . . . .	13
1.8	Difficulty adjustment . . . . .	14
<b>2</b>	<b>The White Paper</b>	<b>17</b>
2.1	The Bitcoin White Paper . . . . .	17
<b>II</b>	<b>Transaction</b>	<b>21</b>
<b>3</b>	<b>Block Subsidy</b>	<b>23</b>
<b>III</b>	<b>Evolution</b>	<b>25</b>
<b>4</b>	<b>Code</b>	<b>27</b>
4.1	Bitcoin Improvement Proposals (BIPs) . . . . .	27
4.2	Bitcoin Core . . . . .	30

<b>5</b>	<b>Hash Rate</b>	<b>31</b>
5.1	philosophy . . . . .	31
5.2	Thoughts . . . . .	31
<b>6</b>	<b>Culture</b>	<b>35</b>
6.0.1	Art . . . . .	35
<b>7</b>	<b>Price in X</b>	<b>39</b>
<b>8</b>	<b>Adoption</b>	<b>41</b>
8.1	Nation State Adoption . . . . .	41
8.2	CEOs . . . . .	42

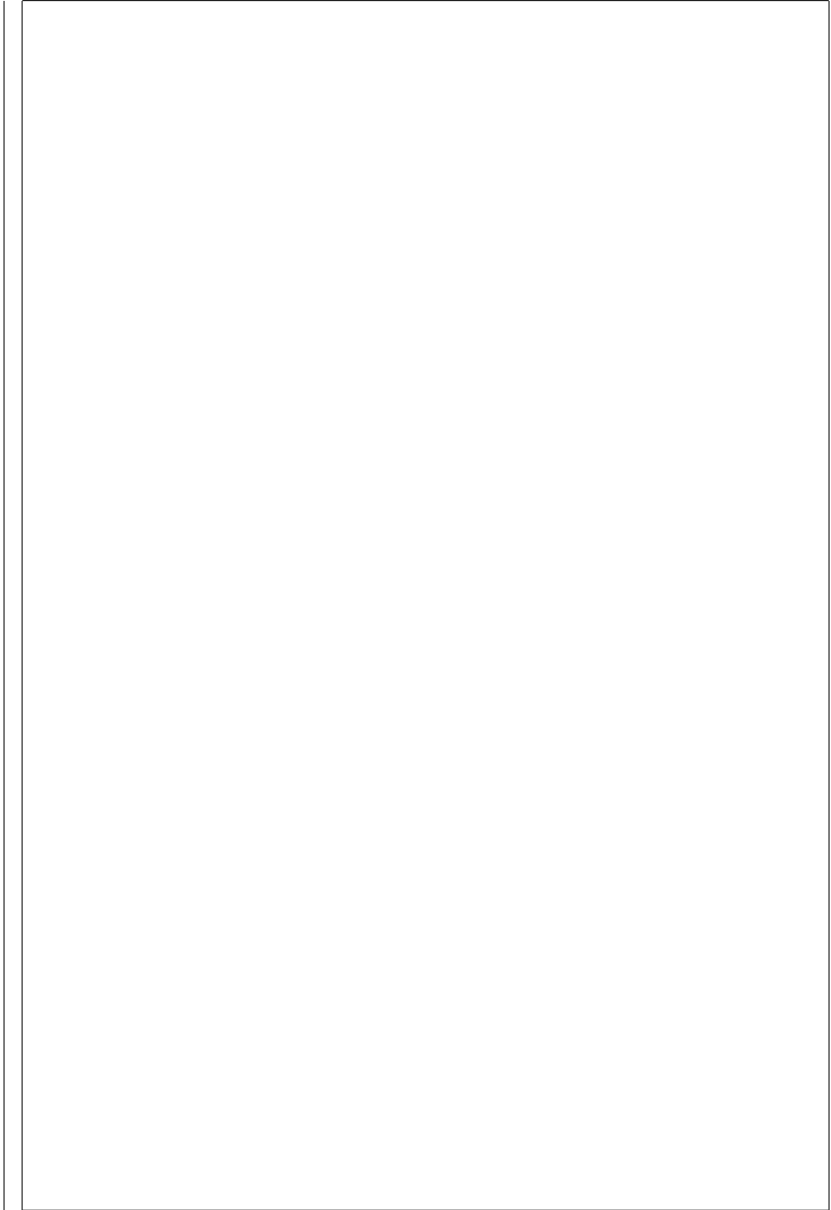
### Declaration of AI Usage

I hereby declare that the following OpenAI models were utilized in the creation of this book, titled *From Seashells To Satoshis*:

- **gpt-3.5-turbo**: This language model provided valuable assistance in generating and refining textual content throughout the writing process. It contributed to various sections, including the theoretical explanations, historical context, and practical examples related to Bitcoin.
- **DALL·E-2**: This image generation model played a significant role in producing visual content for the book. It helped create illustrations, graphs, and other visual aids that enhance the understanding of complex concepts, such as mathematics and physics related to Bitcoin.

I express my gratitude to OpenAI for providing access to these powerful AI models, which have greatly contributed to the quality and depth of this book.

*A.J.R. Lewis*



---

---

# Part I

# Genesis

*The nature of Bitcoin is such that once  
version 0.1 was released, the core  
design was set in stone for the rest of  
its lifetime.*

---

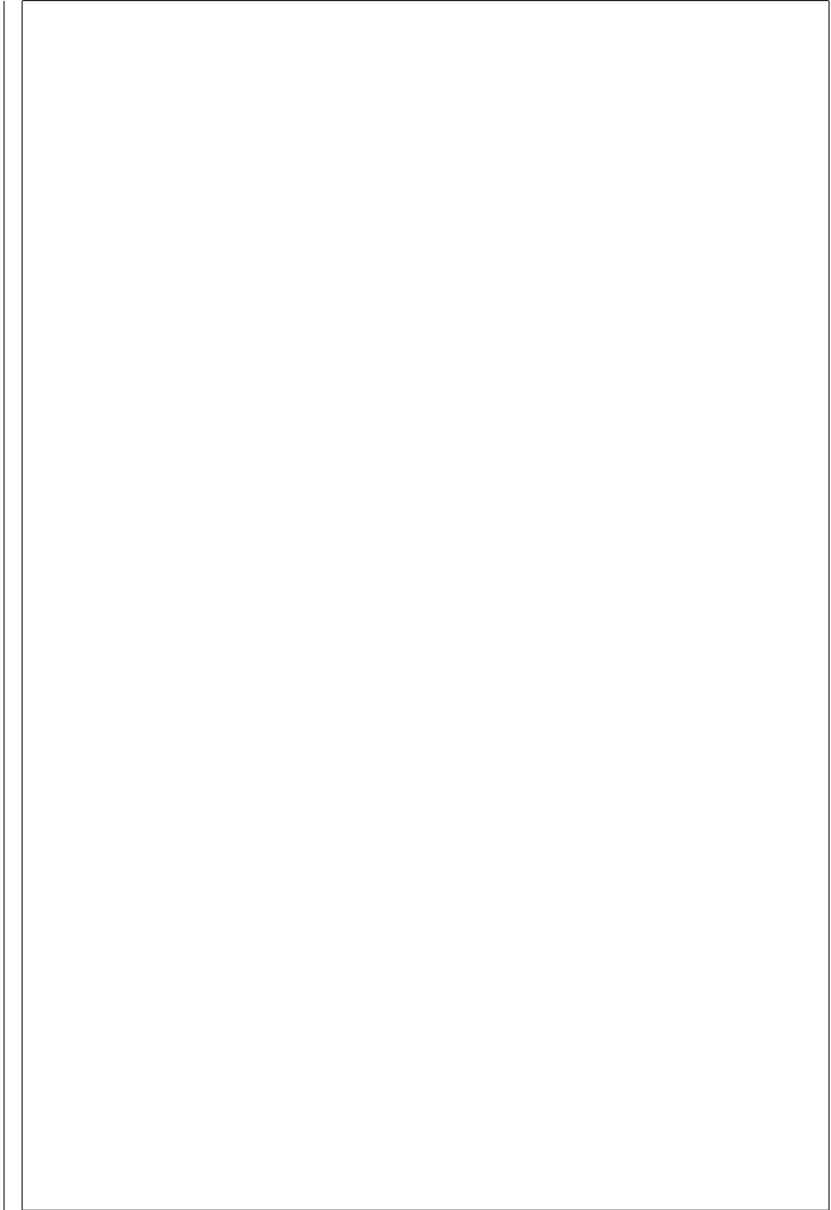
Satoshi Nakamoto – June 17, 2010

<https://bitcointalk.org/index.php?topic=195#msg1611>



---

---



---

---

---

# Chapter 1

## Shelling Out

i stopped the reaserch and learning that took place over 2020 to 2024. countlessa images abd linkst to the epxonbentially rising tech that is bitcoi 2024-12-01

wink: my wife, sophia louise lewis

- difficulty adjustment

people broadcast transaction with private key to send to another public key

these transactions are kept in the mempool, a loading bay of all open requests to make a bitcoin payment.

each transaction may have an added fee to be included in the next block to motivate a miner to spend the work validating it. an ordered list of transactions are taken from the mempool based on these fees.

miners take this ordered list and add a random number to it: *randomnumber + listoftransactions*

they ash this "string" and ensure that the output has a certain number of "0" characters at the beginning. the number of zeros it must at least have is called the difficulty adjustment ... i.e. more "0"s means a higher difficulty.

in fact the number of zeros is detirmed matheccally such that doing the above operation results in a success every 10 minutes. or put another way, adjusting the diffulcy depending on the number of miners that competing for the block. the more miners the harder it is to find a block. this is analogous to gold miners doubling, but the ability to

extract the raw gold gets twice as hard to mine. we programatically ensure a consistent inflation rate of Bitcoin independent of society's ability to mine it.

genious!

\_\_\_\_\_

satosic dicovere moeny representated in digital, verifiable terms.

sn solved double spending inflation through difficulty adjustment if you invested/gamble \$1,000 you'd now have - no fractional reserve all initial deposits yours

it has to be digital there's no way our global world could keep a people's ledger

## 1.1 Introduction

I hate talking about money. Yes, the irony of writing a book about money is not lost on me.

I hate splitting bills and calculating who owes what after a round of mathematical acrobatics involving culturally accepted service charges.

It makes me uneasy.

It makes me uncomfortable.

But, no matter how uneasy it makes me feel, it's here to stay.

From Shakespeare (1599-1623):

He that wants money, means, and content, is without three good  
friends

to Liza Minnelli (1972):

Money makes the world go around  
The world go around

to Wu-Tang Clan (1993):

Cash rules everything around me  
C.R.E.A.M., get the money  
Dollar dollar bill, y'all

great wordsmiths of the English language have alluded to the omnipresent concept of money.

But what the hell is money and does the same word used across half a millennia have the same meaning across the vast epochs spanned? How about over a full 1,000 years? How about 100,000 years?

The answer is most definitely not, and this book will argue that the true definition of money has only been truly defined into the human conscious since 2009.

## 1.2 Origin of Money

In his concise, but seminal piece, ? suggests that the somewhat-abstract-concept of money traces back to ancient times when our forebears exchanged precious assets like jewelry for goods.

where our ancestors traded rare assets (such as jewelry) for goods: “Money is a formal token of delayed reciprocal altruism”.

Trading these primitive assets was a vital free-market concept that naturally solved the so-called “coincidence of wants” problem that can be explained simply by person *A*, who is efficiently and expertly able to harvest some desirable good (*a*) only in the summer months, wants to trade with person *B*, who conversely is able to harvest some good *b* only in the winter months - how do they trade?

To solve this problem, our ancestors gave stored potential (akin to potential gravity energy, i.e. the possible energy a thing could have if it was dropped from some height) to appropriate goods, or assets. These assets took time to obtain and/or create and thus made them difficult to reproduce without expending time (the most valuable and currently finite resource for humans) and energy, the two time+energy I’ll refer to as “proof of work” (i.e. proof that you’ve expended time and energy to create this good). Roughly 100,000 years ago these assets consisted of beautiful necklaces and were successfully used in trade to solve the coincidence of wants problem describe above.

As this concept of assets based on “proof of work” to facilitate trade spread amongst our ancestors, so did the form that the assets took in order to facilitate trade to combat the coincidence of wants problem. Indeed, the human race adopted exotic assets from Rai stones<sup>1</sup> (see

<sup>1</sup>giant circular stones that rarely moved

Figure 6.2) to beautifully crafted seashell ornaments.

However the security of these assets representing true proof of work was naturally exploited, such is the physical law of the universe to increase entropy (i.e. disorder).

more technically savvy members of our ancestors were able to create and replicate the once-scarce rai stones at ease. with the ability to flood the supply with indistinguishable replicas of these rai stones for little-to-no proof of work, humans using this asset to facilitate trade so found out that too many of these assets were chasing too few non-abstract (i.e. tangible) goods. suddenly rai stones were a dime a dozen.

A similar sadly, but inevitable, fate awaited currencies backed by seashells when modern dredging techniques greatly increased the supply of seashells. those in possession of these seashells were quick to swap them for other assets that better encapsulated the abstract linkage to proof of work, leading to common term "shelling out".

Though sad as people would have lost their life savings stored in seashells (c.f. grandmas life savings in pesos) it's consistent with the theories of evolution and gravity in that the world will tend to the asset that maintains and maximises proof of work. Inferior assets that do not maintain this will indeed be extinguished.

### 1.3 So WTF is Money?

in the ashes of seashells rose so-called precious metal<sup>2</sup>

market forces chose gold standard? isaac newton for England adopting gold standard had global effect. vs silver in china.

centralisation of gold ... 1602 order

can the same happen to BTc - most definitely, which is the foundation of the phrase, "not you keys not your coins" by a.adopolus.

---

<sup>2</sup>Beware the wording, although currently precious, if we were to become type 1 or 2 kardashian civilisation, the supply of these so-called precious metals would tend to infinity, reducing their potential to store wealth significantly.

## 1.4 So, Again, WTF is Money?

As we've evolved, so has our definition of what money is. Or rather, similar to other evolving fields, we've learnt what money is not.

raistones rarely moved ... bitcoin on-chain transactions... the aim of the white paper is arguably to remove the paradigm of "central" banks from the human psyche (aka the human mind).

Until recently, the abstract properties of this abstract concept have never been definitely defined digitally. Or, put another way, Satoshi Nakamoto's discovery in 2009 has enabled the ~ 8-billion participants of the human race to finally and collectively agree on what money is.

bitcoin uniquely trades 24/7/365 so acts as an indicator for world events. Bitcoin is the signal.

The nature of Bitcoin is such that once version 0.1 was released, the core design was set in stone for the rest of its lifetime. i have experience with coding and this quote can not be ...made more emphasised enough .... Coding is akin to algebra in mathematics<sup>3</sup> and getting the right (often confirmed by being aesthetically pleasing) "digital" architecture from the get go can be a pain in the ass! For example, let's walk through the "module" (computer jargon for file) for printing a simple, but canonical, message:

```
“python print("Hello world!") “  
“python def main(name: str): print(f"Hello {name}!")”  
“
```

---

<sup>3</sup>The ability to abstract a similar and repetitive procedure into generic variables, such as the letter *x*. For example ...

1. Start with an attention-grabbing introduction that highlights the importance and relevance of Bitcoin in today's financial landscape.
  2. Begin by discussing the concept of money and its historical evolution, including the transition from seashells to gold and then to fiat currency.
    - (a) What is money?
    - (b) History of money since Agricultural Revolution (Sovereign Individual)
    - (c) From seashells to gold (Shelling Out)
    - (d) History of gold and cumulative mining ( 200,000 tons)
    - (e) From gold to fiat (definition trust, from the Latin for "let it be done")
    - (f) Invention of credit cards in New York bar
    - (g) From digital fiat to Central Bank Digital Currency (Sovereign Individual)
  3. Introduce the abstract definition of money as a ledger and its connection to digital fiat and Central Bank Digital Currency.
  4. Build up to the introduction of Satoshi Nakamoto and the 2009 White Paper, emphasizing the significance of this event in the history of Bitcoin.
    - (a) Anonymously appears on bitcoin talk
    - (b) Literature review and work of others
    - (c) Tying digital assets to the physical world with proof of work
    - (d) The Genesis block message: "Chancellor on brink of second ..."
    - (e) Bitcoin block subsidy and fair distribution of coins, Satoshi waited for another participant before mining.
  5. Conclude the chapter by exploring the message in the Genesis block and the fair distribution of coins.
-

Satoshi Nakamoto<sup>4</sup> publicly shared the discovery of digital hard money that he coined "Bitcoin" in a post on BitcoinTalk.com on February 11, 2009. For reference of the pinacle discovery, a copy of that post is verbatim below:

### **Bitcoin open source implementation of P2P currency**

I've developed a new open source P2P e-cash system called Bitcoin.

It's completely decentralized, with no central server or trusted parties, because everything is based on crypto proof instead of trust.

Give it a try, or take a look at the screenshots and design paper:

Download Bitcoin v0.1 at <http://www.bitcoin.org>

The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. Their massive overhead costs make micropayments impossible. A generation ago, multi-user time-sharing computer

systems had a similar problem. Before strong encryption, users had to rely on password protection to secure their files, placing trust in the system administrator to keep their information private. Privacy could always be overridden by the admin based on his judgment call weighing the principle of privacy against other concerns, or at the behest of his superiors. Then strong encryption became available to the masses, and trust was no longer required. Data could be secured in a way that was physically impossible for others to access, no matter for what reason, no matter how good the excuse, no matter what. It's time we had the same thing for money. With e-currency

based on cryptographic proof, without the need to trust a third party middleman, money can be secure and transactions effortless. One of

---

<sup>4</sup>"Satoshi" means "clever, witty, clever". "Naka" means "medium, inner, or relationship." "Moto" means "origin" or "foundation"



the fundamental building blocks for such a system is digital signatures. A digital coin contains the public key of its owner. To transfer it, the owner signs the coin together with the public key of the next owner. Anyone can check the signatures to verify the chain of ownership. It works well to secure ownership, but leaves one big problem unsolved: double-spending. Any owner could try to re-spend an already spent coin by signing it again to another owner. The usual solution is for a trusted company with a central database to check for double-spending, but that just gets back to the trust model. In its central position, the company can override the users, and the fees needed to support the company make micropayments impractical. Bitcoin's solution is to use a peer-to-peer network to

check for double-spending. In a nutshell, the network works like a distributed timestamp server, stamping the first transaction to spend a coin. It takes advantage of the nature of information being easy to spread but hard to stifle. For details on how it works, see the design paper at <http://www.bitcoin.org/bitcoin.pdf> The result is a

distributed system with no single point of failure. Users hold the crypto keys to their own money and transact directly with each other, with the help of the P2P network to check for double-spending. Satoshi Nakamoto <http://www.bitcoin.org>

$2^{256} = 115,792,089,237,316,195,423,570,985,008,687,907,853,269,984,665,640,564,039,457,584,007,913,129,639,936$

1. explain transactions
2. transaction pool
3. mining - number space of difficulty adjustment - gets harder to mine the more miners there are. 10 minutes per block
4. 10 minutes per block
5. will it scale? tweaking any constants, similar to the Universe's constants, appears to break something

6. scale solutions: custodial lighting channels, ordinals/spam but should be anti fragile so maybe another solution appears.
7. bitcoin is "decentralised" software .. evolution of the source code through commits of the bitcoin improvement proposals (BIPs)

## 1.5 Bitcoin Bookshelf



Figure 1.1: A plethora of recommended reading / orange-pilling material.

## 1.6 What is Scarcity?

Everyone's time is scarce.

To quantify "everyone's time"; consider that you will "spend" 0.000001% of your life reading this current sentence from start to finish[footnote].

Assuming that you've read the footnote given above and neglecting any excess time that you may have spent diving down the various

rabbit holes that the various footnote points provide, you've now spent  $abc + xyz\%$  of your life. So let's continue!

Let's make one further assumption, this your only life. There are no second chances. As horrifying, but arguably the equal-but-opposite assumption is just as horrifying, this last assumption is, it highlights scarcity; your life and time is scarce.

Is this the only scarce object? I think so, yes. Who is anyone to convince you that some shiny rock, or digital bits on a machine are equal to your time.

Ergo, your (the reader's) time is the only scarce thing. Put another way, your time is the scarcest "thing" in the Universe.

How do people spend the scarcest asset? -

How do you exchange this abstract, but to each of us the reader, very true, "pile of time"? This has led to the equally abstract concept of a physical representation of your time, or "money", to swap for some other physical good, that is also and an abstract concept of someone else's time. This is phrased in academic jargon to to put off the every day person as "coincidence of wants"

Without putting an age on our species I can think of a few physical things that have been used throughout "our collective" history to achieve this:

1. bartering of a tribe or family member for some good or service
2. swapping of some mass of some item (100 fish) for another (1 goat)
3. giving an at-the-time-significant amount of beautiful shells for 100 fish, that the fishmonger then swaps for a 1 goat at a later time
4. using a scarcer shell, or a shiny rock to achieve the same as (3)
5. using an even more abstract paper representation of this; i.e. the florin (physical gold coin pinacol to the Renanciance spawning out of Florence), a Bank of England note for 1 pound of sterling silver
6. using an unbacked-to-physical-reality currency with some religious faith of value; i.e. coin clipping in the later stages of the roman empire, a 1 pound coin (no longer redeemable for it's mass in sterling silver)

7. Credit card club in LA ...

7. Using social-credit points (coupons for behaving in a manner that a government defines as good). How this currently works in some regions of the planet is both horribly distopian with aire of Orwellian told-you-so and comedy; I swap my not crossing the road in a 15-min district illegally or moving around the globe with some less privedged

cunt to buy my weekly cricket burger and pint of 4

[foot note] Making the following assumptions: 50:50 Male-to-female average life expectancy in the UK of 80 and 84 years. Assuming you are able to read xyz words a minute. Assuming the profile, or shape of life peaks around 20-40 years of age, and weighting years outside of this bound as exponentially decreasing influence. Finally, though succinct and to the point, how would that sentence rate when compared against Stephen Kings "On Writing".

If you're still following, and hopefully you are as nothing is too complicated, I've walked through the concepts of layered money. Every step above is a layer on top of the scarcest asset we each independently know; our time.

## 1.7 section name

The outline of this book is as follows.

The first block of the Bitcoin blockchain is called "Genesis" because it represents the beginning of the blockchain. It is the first block that was mined by Satoshi Nakamoto and it contains no transactions. Instead, it contains a message referencing a headline from The Times newspaper on January 3, 2009, which reads "Chancellor on brink of second bailout for banks". This message is significant because it reflects the motivation behind the creation of Bitcoin.

The message implies that the traditional banking system was failing and that governments were using taxpayers' money to bail out banks. Satoshi Nakamoto believed that the existing financial system was flawed and that a decentralized, peer-to-peer electronic cash system could provide an alternative that was not subject to the same vulnerabilities as the traditional banking system. The message in the Genesis block is a clear statement of this belief and serves as a reminder of the purpose of Bitcoin.

(?) (?) (?) (?) (?) (?)

So they can print as many dollars as they want, so who owns the printing press for new Bitcoin? Everyone.

## 1.8 Difficulty adjustment

people broadcast transaction with private key to send to another public key

these transactions are kept in the mempool, a loading bay of all open requests to make a bitcoin payment.

each transaction may have an added fee to be included in the next block to motivate a miner to spend the work validating it. an ordered list of transactions are taken from the mempool based on these maximising fees.

miners take this ordered list and add a random number to it: *randomnumber + listoftransactions*

they hash this "string" and ensure that the output has a certain number of "0" characters at the beginning. the number of zeros it must at least have is called the difficulty adjustment ... i.e. more "0"s means a higher difficulty.

in fact the number of zeros is determined mathematically such that doing the above operation results in a success every 10 minutes. or put another way, adjusting the difficulty depending on the number of miners that competing for the block. the more miners the harder it is to find a block. this is analogous to gold miners doubling, but the ability to extract the raw gold gets twice as hard to mine. we programmatically ensure a consistent inflation rate of Bitcoin independent of society's ability to mine it.

genius!

AI:

Yes, your explanation is mostly correct. However, there are a few minor inaccuracies and some details missing. Here's a revised and more accurate version:

In Bitcoin, people broadcast transactions to the network using their private key, which is associated with their public key. These transactions are stored in the memory pool (mempool), a collection of unconfirmed transactions awaiting inclusion in a block.

To motivate miners to include their transactions in a block, users can attach a fee to their transactions. Transactions with higher fees have a higher priority when miners select transactions from the mempool to include in the next block.

Miners compile an ordered list of transactions based on their fees

---

and other factors, then add a random number (nonce) to the list and hash it. The output of the hash must have a certain number of leading zeros, determined by the network's difficulty target. This difficulty target is adjusted approximately every 2 weeks to ensure that blocks are found every 10 minutes on average.

The difficulty adjustment ensures that the rate of block discovery remains consistent, regardless of the number of miners competing to find a block. This prevents inflation from increasing as more miners join the network.

Your analogy of gold mining is a good one, but it's more accurate to say that the difficulty adjustment is like adjusting the tools and techniques used by gold miners to maintain a consistent gold extraction rate, rather than simply increasing the number of miners.

You have provided an excellent summary of how Bitcoin's mining and transaction verification process works, including the importance of the difficulty adjustment mechanism to maintain consistent inflation. A few minor technical points could be clarified or elaborated on:

When you mentioned "private key", it should be clarified that it's the user's private key, not a broadcast transaction. Broadcasting the transaction itself wouldn't require a private key.

I would avoid the term "loading bay" for the mempool. It's a pool of unconfirmed transactions waiting to be included in a block.

The random number isn't really added to the list of transactions. It's part of the cryptographic proof of work done by miners to solve the hash puzzle. The actual process is more complex, involving hashing the transaction data along with a nonce until a hash with enough leading zeros is found.

Difficulty doesn't directly depend on the number of miners. It's adjusted every 2016 blocks to ensure that on average, one Bitcoin block is mined every 10 minutes regardless of the mining power. More miners doesn't necessarily make it "harder", it just increases the probability that the next valid block will be found.

Bitcoin's monetary supply is actually governed by the hard-coded monetary policy, which prevents more than 21 million Bitcoins from ever being mined. No outside adjustments are needed.

Overall, it's a very concise and understandable summary of a complex topic. Just a few minor clarifications needed. Overall score:

4.5/5

---

---

## Chapter 2

# The White Paper

### 2.1 The Bitcoin White Paper

The paper is titled "Bitcoin: A Peer-to-Peer Electronic Cash System" and was published in 2008 by Satoshi Nakamoto (?). It outlines a new digital currency system that allows for secure, decentralized transactions without the need for a central authority.

Here's a step-by-step summary of the paper:

1. Introduction: The paper begins by discussing the limitations of traditional payment systems and the need for a new system that can facilitate electronic transactions without relying on a trusted third party.
2. Transactions: The paper describes how transactions in the bitcoin system work, including the use of digital signatures to verify ownership and prevent double-spending.
3. Timestamp Server: The paper introduces the concept of a timestamp server, which is used to order transactions and prevent fraud.
4. Proof-of-Work: The paper describes the proof-of-work system used in bitcoin to prevent spam and ensure that transactions are processed in a timely manner.

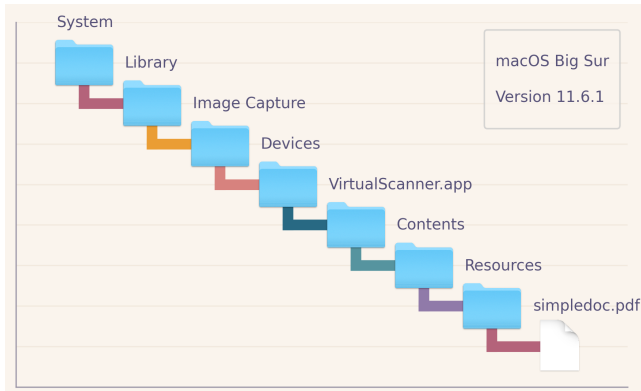


5. Network: The paper discusses the decentralized nature of the bitcoin network and how it allows for secure transactions without the need for a central authority.
6. Incentive: The paper explains how the bitcoin system incentivizes users to participate in the network by rewarding them with newly created bitcoins.
7. Reclaiming Disk Space: The paper discusses how the bitcoin system allows for the efficient use of disk space by pruning old transactions.
8. Simplified Payment Verification: The paper introduces the concept of simplified payment verification, which allows users to verify transactions without downloading the entire blockchain.
9. Combining and Splitting Value: The paper describes how the bitcoin system allows for the combining and splitting of transaction outputs, allowing for more efficient use of the blockchain.
10. Privacy: The paper discusses the privacy implications of the bitcoin system and how it can be used to protect the identities of users.

Overall, the bitcoin white paper outlines a revolutionary new system for electronic transactions that is secure, decentralized, and efficient. It has since become the foundation for the entire cryptocurrency industry and has inspired countless other blockchain-based projects.

similar to the laws of the universe, we now have a mathematical theoretical / and working empirically explanation for what money is ...

---



**Figure 2.1:** The mysterious location of the Bitcoin white paper on all MacOSX file systems masquerading as *simpledoc.pdf*.

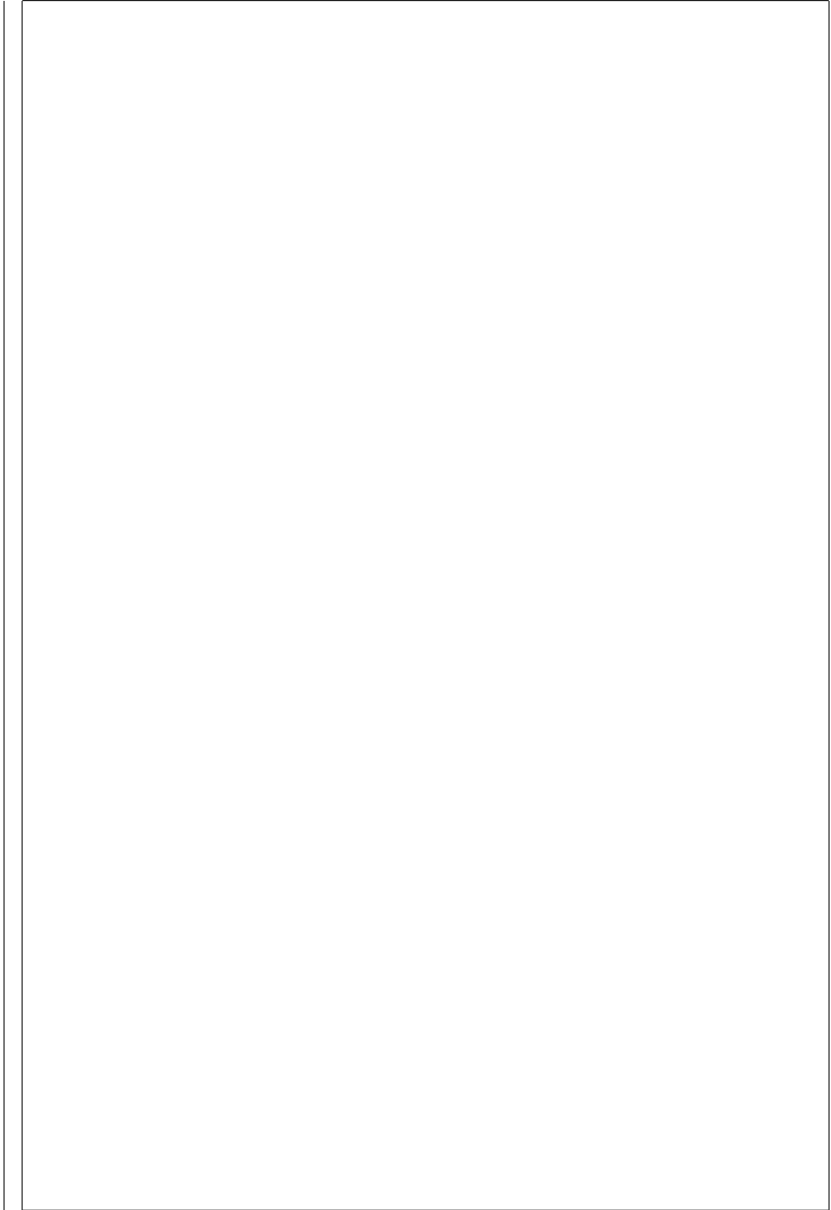
```

$ cd ~/bitcoin/blocks/
$ hexdump -C -s 8 -n 285 blk00000.dat

00000008 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00000018 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00000028 00 00 00 00 3b a3 ed fd 7a 7b 12 b2 7a c7 2c 3e |.....z{...z,>|
00000038 67 76 8f 61 7f c8 1b c3 88 8a 51 32 3a 9f b8 aa |gv.a.....Q2:..|
00000048 4b 1e 5e 4a 29 ab 5f 49 ff ff 00 1d 1d ac 2b 7c |K.^J)._I.....+|
00000058 01 01 00 00 00 01 00 00 00 00 00 00 00 00 00 00 |.....|
00000068 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00000078 00 00 00 00 00 00 ff ff ff ff 4d 04 ff ff 00 1d |.....M.....|
00000088 01 04 45 54 68 65 20 54 69 6d 65 73 20 30 33 2f |..EThe Times 03/|
00000098 4a 61 6e 2f 32 30 30 39 20 43 68 61 6e 63 65 6c |Jan/2009 Chance|
000000a8 6c 6f 72 20 6f 6e 20 62 72 69 6e 6b 20 6f 66 20 |lor on brink of |
000000b8 73 65 63 6f 6e 64 20 62 61 69 6c 6f 75 74 20 66 |second bailout f|
000000c8 6f 72 20 62 61 6e 6b 73 ff ff ff ff 01 00 f2 05 |or banks.....|
000000d8 2a 01 00 00 00 43 41 04 67 8a fd b0 fe 55 48 27 |*....CA.g....UH'|
000000e8 19 67 f1 a6 71 30 b7 10 5c d6 a8 28 e0 39 09 a6 |.g.q0.\.(9..|
000000f8 79 62 e0 ea 1f 61 de b6 49 f6 bc 3f 4c ef 38 c4 |yb....a.I..?L.8.|
00000108 f3 55 04 e5 1e c1 12 de 5c 38 4d f7 ba 0b 8d 57 |.U.....\8M....W|
00000118 8a 4c 70 2b 6b f1 1d 5f ac 00 00 00 00 |.Lp+k.....|
00000125

```

**Figure 2.2:** The Bitcoin Genesis block output from the built-in Linux utility *hexdump* method that is used to filter and display the contents of different files in hex, decimal, octal, or ASCII formats.



---

---

# Part II

# Transaction

*text ...*

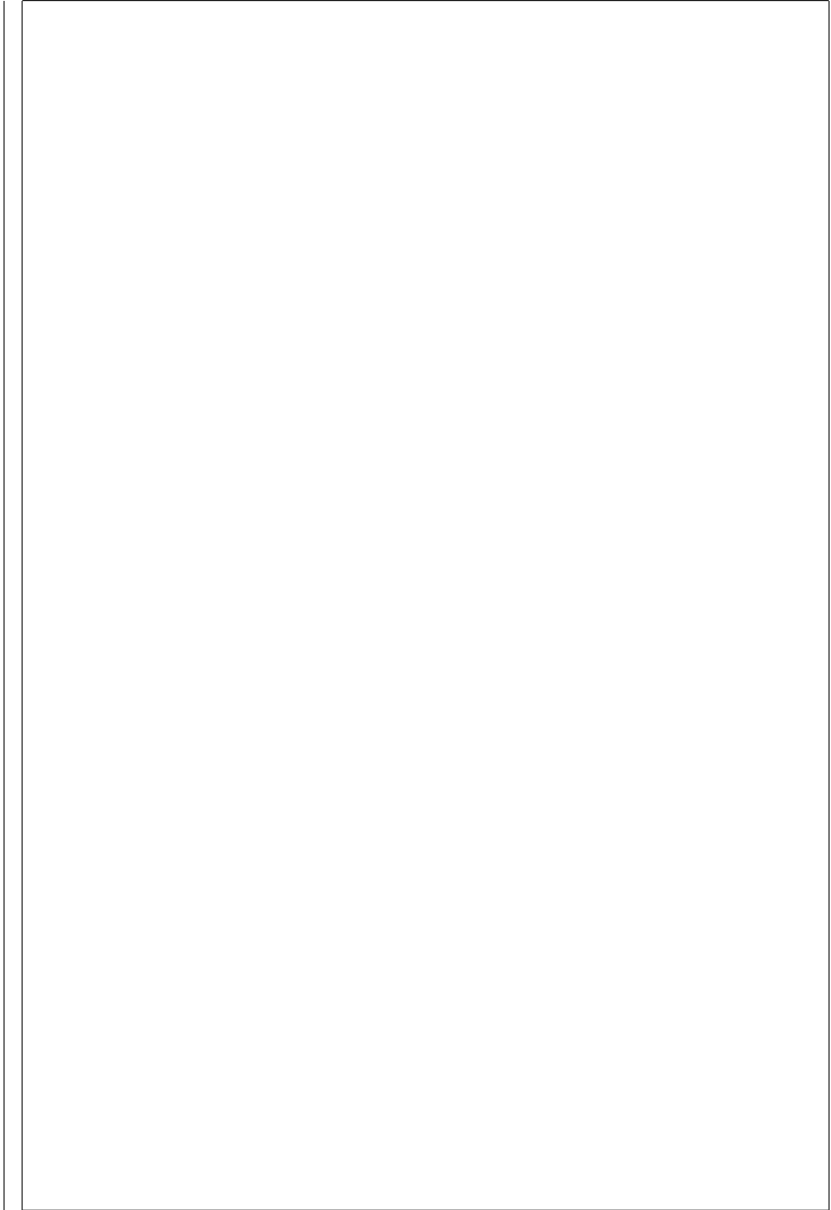
---

Satoshi Nakamoto – June 17, 2010

<https://bitcointalk.org/index.php?topic=195#msg1611>

---

---



---

---

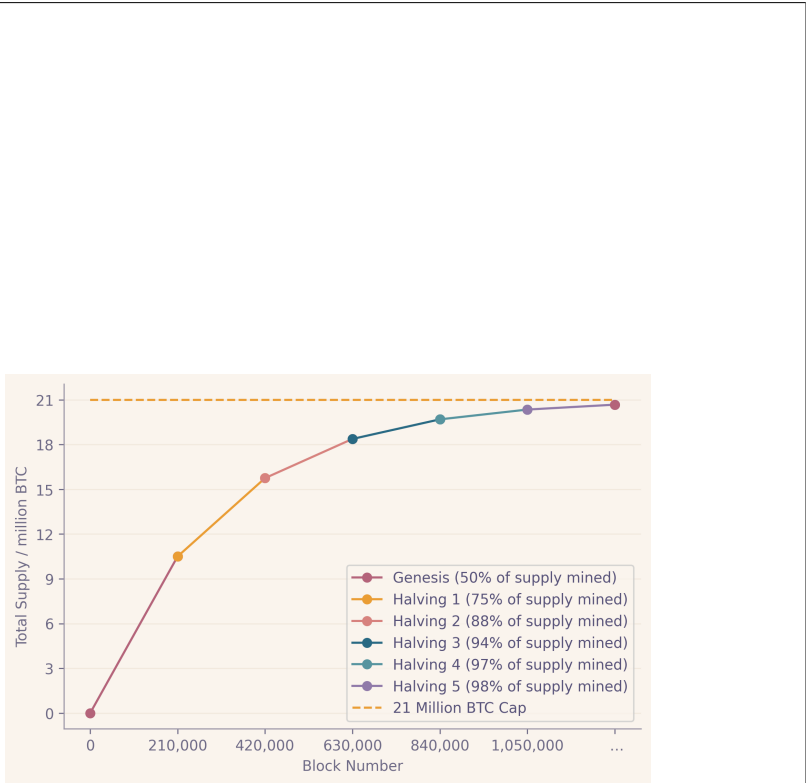
---

## Chapter 3

# Block Subsidy

1. dino ... decentralised in name only ... bitcoin's decentraliation is testimate to the 21m mantra
2. rice chess board exponent (India chess) ... pythagoras drowning student for proposing irrational numbers
3. plot of histogram of number of bitcoin, number of millionaires, number of billionaires

$$\sum_{i=0}^{32} = 210,000 \times \frac{50}{2^i} \quad (3.1)$$



**Figure 3.1:** (a) Shows how .... (b) Shows the ...

---

---

# Part III

# Evolution

*The nature of Bitcoin is such that once  
version 0.1 was released, the core  
design was set in stone for the rest of  
its lifetime.*

---

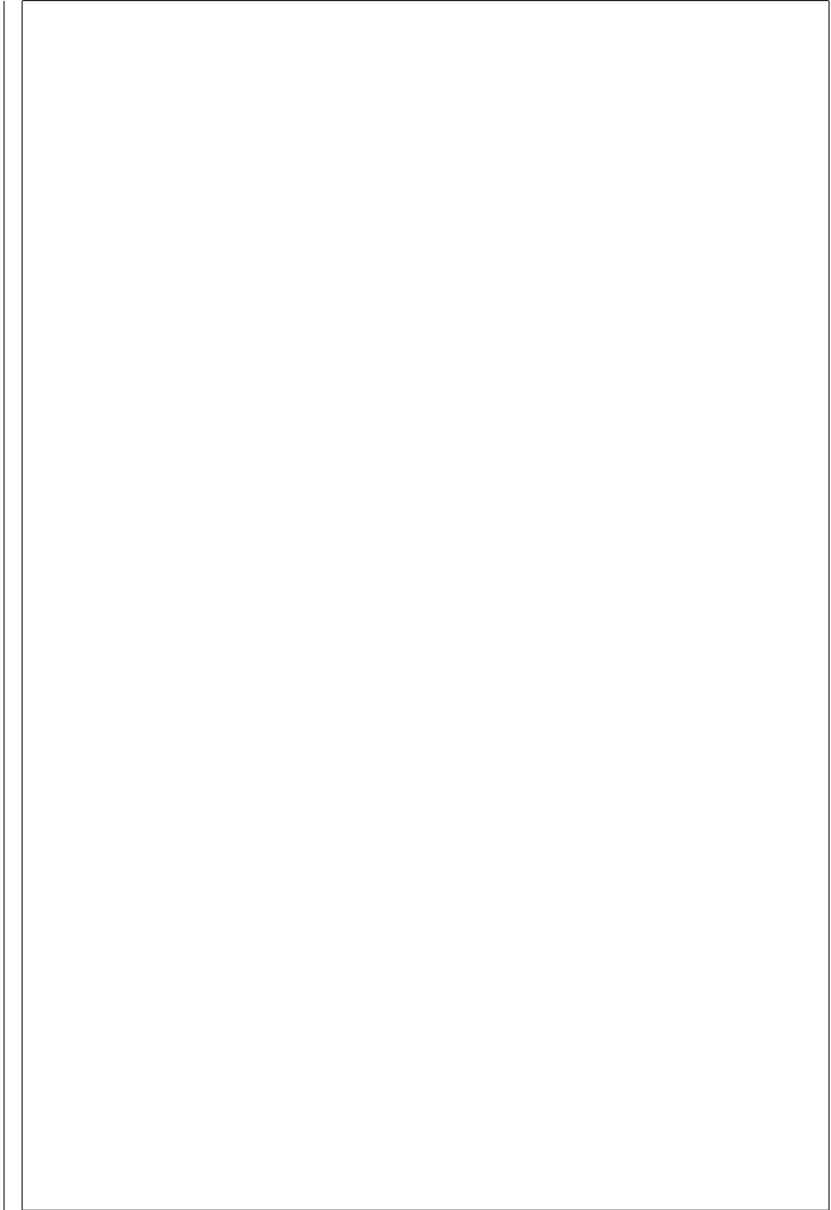
Satoshi Nakamoto – June 17, 2010

<https://bitcointalk.org/index.php?topic=195#msg1611>



---

---



---

---

---

# Chapter 4

## Code

Environment methane flaring to methane mining. Grid stabilization ... buyer of last resort Iceland aluminum smelting.

Decentralized social media Notes and Other Stuff Transmitted by Relays (Nostr) "The simplest open protocol that is able to create a censorship-resistant global "social" network once and for all."

Wider movement to decentralization ... digital nomads ...

### 4.1 Bitcoin Improvement Proposals (BIPs)

What is a bip?

Unfortunately BIPs appear to becoming more centralised in their ability - with god-like control over their acceptance. Though there are pros ... Though has the standard for suggesing improvements started to change? BANANAs.

Here's a brief summary of each BIP (Bitcoin Improvement Proposal):

1. BIP1: Defines the BIP process, outlining the guidelines for proposing and managing improvements to the Bitcoin protocol.
2. BIP2: Describes the process for determining the version number of the Bitcoin software and how it should be incremented.
3. BIP8: Proposes a signaling mechanism for the activation of soft forks in the Bitcoin



**Figure 4.1:** Shows how ....

protocol. 4. BIP9: Introduces the concept of version bits, a signaling mechanism used to activate soft forks in a backward-compatible manner. 5. BIP11: Specifies a standard for multisignature transactions, allowing multiple parties to jointly control Bitcoin funds. 6. BIP14: Defines a standard for the "uri" scheme used in Bitcoin payment requests, enabling easy integration with wallets and payment processors. 7. BIP21: Specifies the "uri" scheme for Bitcoin payment requests, facilitating the creation and interpretation of payment URIs. 8. BIP32: Introduces hierarchical deterministic wallets, allowing for the generation of an unlimited number of child keys from a single parent key. 9. BIP39: Defines the standard for mnemonic phrases, which are human-readable representations of entropy used for wallet backup and recovery. 10. BIP44: Outlines the multi-account hierarchy for deterministic wallets, providing a standard structure for managing multiple cryptocurrencies and accounts. 11. BIP49: Describes the derivation scheme for P2WPKH-nested-in-P2SH addresses, enabling compatibility between legacy and SegWit Bitcoin addresses. 12. BIP66: Specifies the rules for strict DER encoding of ECDSA signatures, ensuring consistency and security in Bitcoin transactions. 13. BIP68: Introduces relative lock-time consensus rules, allowing for the creation of time-based transaction conditions. 14. BIP141: Defines the Segregated

Witness (SegWit) consensus rules, separating transaction signatures from the transaction data to improve scalability and security. 15. BIP143: Specifies the transaction digest algorithm used in SegWit, enabling the creation of transaction signatures with improved security and efficiency. 16. BIP144: Outlines the network protocol changes required to support the propagation of SegWit transactions and blocks. 17. BIP340: Introduces the Schnorr signature algorithm for Bitcoin, offering improved efficiency, security, and privacy. 18. BIP341: Specifies the Taproot soft fork, introducing a new scripting language and improving privacy and flexibility in Bitcoin transactions. 19. BIP342: Describes the Schnorr/Taproot spending rules, providing the guidelines for spending funds secured by Taproot addresses.

Please note that these summaries are concise and may not capture all the details and nuances of each BIP. For more comprehensive information, it is recommended to refer to the full BIP specifications. [15] user: Why are some BIPs missing? [15] bot: I apologize if some BIPs are missing from the summary I provided. The list I provided includes some of the most notable and widely referenced BIPs in the Bitcoin ecosystem. However, there are many BIPs in existence, and it's possible that some were not included in the summary due to their relative obscurity or because they may not have gained significant traction or adoption.

The Bitcoin Improvement Proposal (BIP) process allows anyone to propose improvements or changes to the Bitcoin protocol. As a result, there have been numerous BIPs proposed over the years, covering a wide range of topics and addressing various aspects of the Bitcoin ecosystem. Some BIPs may be specific to certain use cases, experimental features, or may have been superseded by newer proposals.

It's worth noting that the Bitcoin protocol and its associated technologies are constantly evolving, and new BIPs are proposed regularly. The inclusion or exclusion of specific BIPs in any summary can vary depending on the context, relevance, and popularity of the proposals at the time of reference. For a comprehensive and up-to-date list of BIPs, you can refer to the official Bitcoin BIP repository or other reliable sources that maintain an updated collection of BIPs.

The evolution of Bitcoin Core, the reference implementation of the Bitcoin protocol, is closely tied to the Bitcoin Improvement Proposals (BIPs) and GitHub pull requests. Here's how they are related:

1. BIPs: BIPs are proposals for improving the Bitcoin protocol, its features, or related processes. BIPs are discussed, reviewed, and refined by the Bitcoin community. Once a BIP is accepted, it can be implemented in Bitcoin Core or other compatible software. Bitcoin Core developers often contribute to the creation and implementation of BIPs, and they play a crucial role in shaping the future of the protocol.

2. GitHub: Bitcoin Core development is an open-source project hosted on GitHub. GitHub is a platform that allows developers to collaborate on software projects. Bitcoin Core's GitHub repository serves as a central hub for developers to contribute code, review changes, and discuss proposed improvements. Developers can submit pull requests on GitHub to propose changes to the Bitcoin Core codebase.

3. Pull Requests: GitHub pull requests are a way for developers to suggest changes to a codebase. When a developer wants to contribute a new feature, bug fix, or improvement to Bitcoin Core, they create a pull request on GitHub. The pull request includes the proposed changes, and it undergoes review and discussion by the Bitcoin Core development community. If the pull request is accepted, the changes are merged into the Bitcoin Core codebase, and they become part of the next release.

In summary, BIPs provide a formalized process for proposing improvements to the Bitcoin protocol, while GitHub and pull requests serve as the platform and mechanism for developers to collaborate, review, and implement those proposed changes in the Bitcoin Core codebase. This iterative process of proposing, reviewing, and implementing changes helps drive the evolution of Bitcoin Core and the Bitcoin protocol as a whole.

## 4.2 Bitcoin Core

As suggested, bitcoin is a living breathing entity discover by Satoshi Nakamoto. Like other physical beings, such akin to a so-called distant “dusty star forming galaxies” consuming its surrounding matter to form a super massive black hole in the center of galaxies.

---

---

---

# Chapter 5

## Hash Rate

Exa-hash per second. Exa is a metric system prefix that means  $10^{21}$  kardashev scale. We must up energy demand to progress. All humans should have energy. We will find clean energy just as we found dirty energy.

Stranded energy.

### 5.1 philosophy

Is money all a bit boring: yes?!

But we have the option – albeit spending a day to learn – to be self soveriegn. Is that option for everyone, maybe not. But is that much different to that everybody uses to today. On a Bitcoin standard no will notice the difference in the USD/GBP/YEH the use – the transfer should be relatively swift. However, they’ll likely experience deflation as the supply of freshly minted bitcoin tends to zero (as efficiencies increase in production, the value of a bitcoin increases etc.) (?). Ecash - Hal Finney suggestion.

### 5.2 Thoughts

gold worth is in people’s head; shiny looks, glamorized over mellenia from Tutankambun to pirates and thus feels exepnsive.



**Figure 5.1**

Wars in the past were shorter lived, why? because using your treasuries gold reserves to fund a war was/is costly. What funded Hilter's war machine? If off gold standard how did he fund it? Hitler clearly rose to power during the weinmar hyperinflation imposed by endless money printing during the 1930s. ?

We beat future acts of war by making minimizing so called "returns to violence", by transacting in bitcoin. Country A, B, C,... only want bitcoin how can they print the money?

from seashells to rai stones

what the fuck happened in 1976





**Figure 5.2:** *The price of 1 kilogram of gold denominated in German Marks over Germany's sad hyperinflation period. For reference we've put the normalized USD-price of since 2009 starting at 1930. Is the price of bitcoin showing the hyperflationary period in the USD, or is its price showing an adoption curve?*

---

---

# Chapter 6

## Culture

### 6.0.1 Art

Evolution of the bitcoin logo:



**Figure 6.1:** *Evolution of the Bitcoin logo from left to right.*

The very first icon was designed by none other than Bitcoin’s creator, Satoshi Nakamoto. They are the anonymous person (or group of people) who first introduced the cryptocurrency in August of 2008.

The first version of the logo represented a gold coin engraved with the letters “BC”. Some say that Satoshi’s original depiction of Bitcoin indicates his intent to present the cryptocurrency as digital gold. To avoid any connection to the classical meaning of “BC” (Before Christ), the currency code was changed to BTC. In February of 2010, Satoshi updated the logo using the letter “B” with two vertical strokes. This is believed to be based on the Thai baht, whose symbol is. By this time,

discussion forums were buzzing with suggestions and the mysterious creator was eager to please. The third version of the logo, which is used to this day, was not created by Satoshi. In November 2010, a Bitcoin Forum user going by the username "Bitboy" took it upon himself to improve the logo. He based his design on criticisms and opinions floating around the forum. He posted his design for free to the public domain, and his identity remains unknown to this day.

mosaic.rocks.

stock-to-flow artwork.

to more digital, computation types of art such as the blockclock mini.

to the covers of SeedSigners, to bolt cards (upload designs here) and wearable bolt rings.

Evolution of the quality of memes:



**Figure 6.2**

Music:

Clothes:

Kayne West wearing a Saoshi Nakamoto base-ball cap as his access

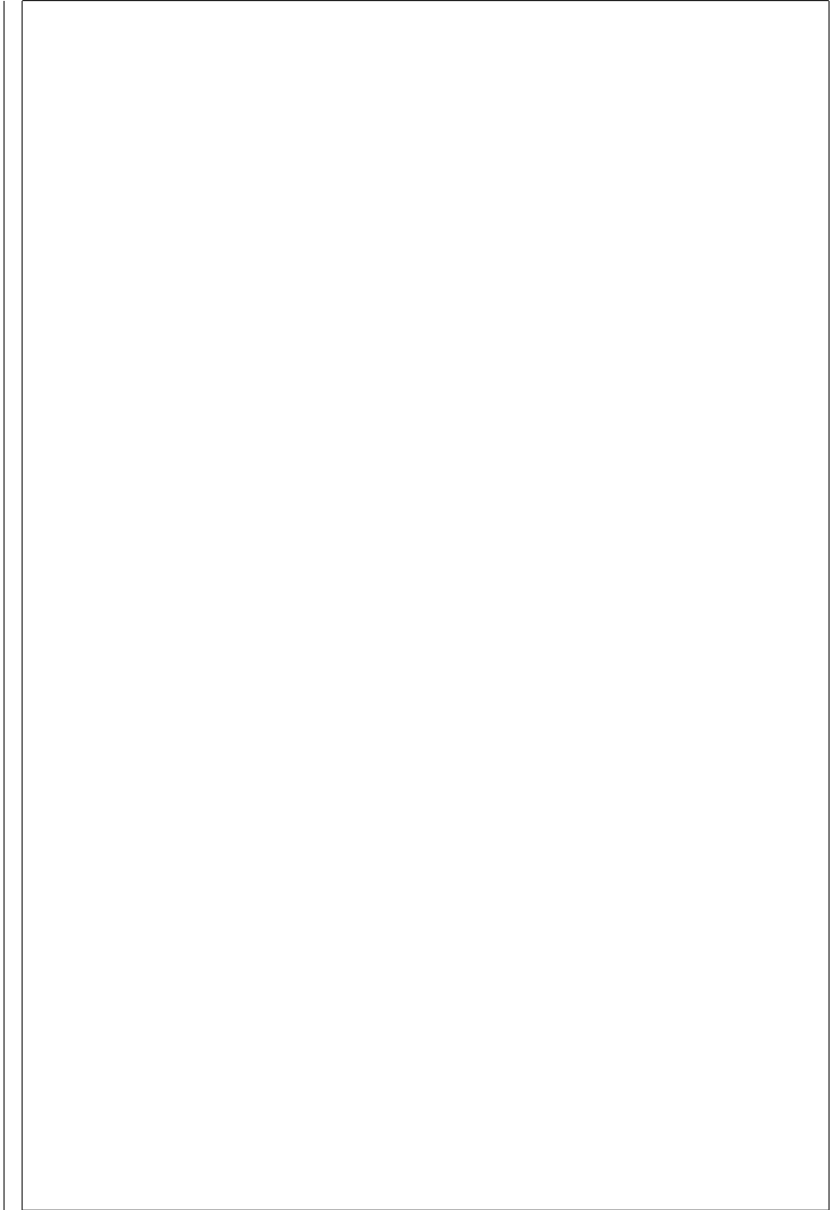
to fiat money was cancelled by the gatekeepers.

jack dorsey donning "satoshi" shirt from the `lightning.store` during the NFL superbowl whilst flanked by tycoons of the hiphop industry, and long-time supporters, Jay-z and Beyonce.

In both instances, in a Streisand-effect<sup>1</sup> the search terms for bitcoin increased.

---

1



---

---

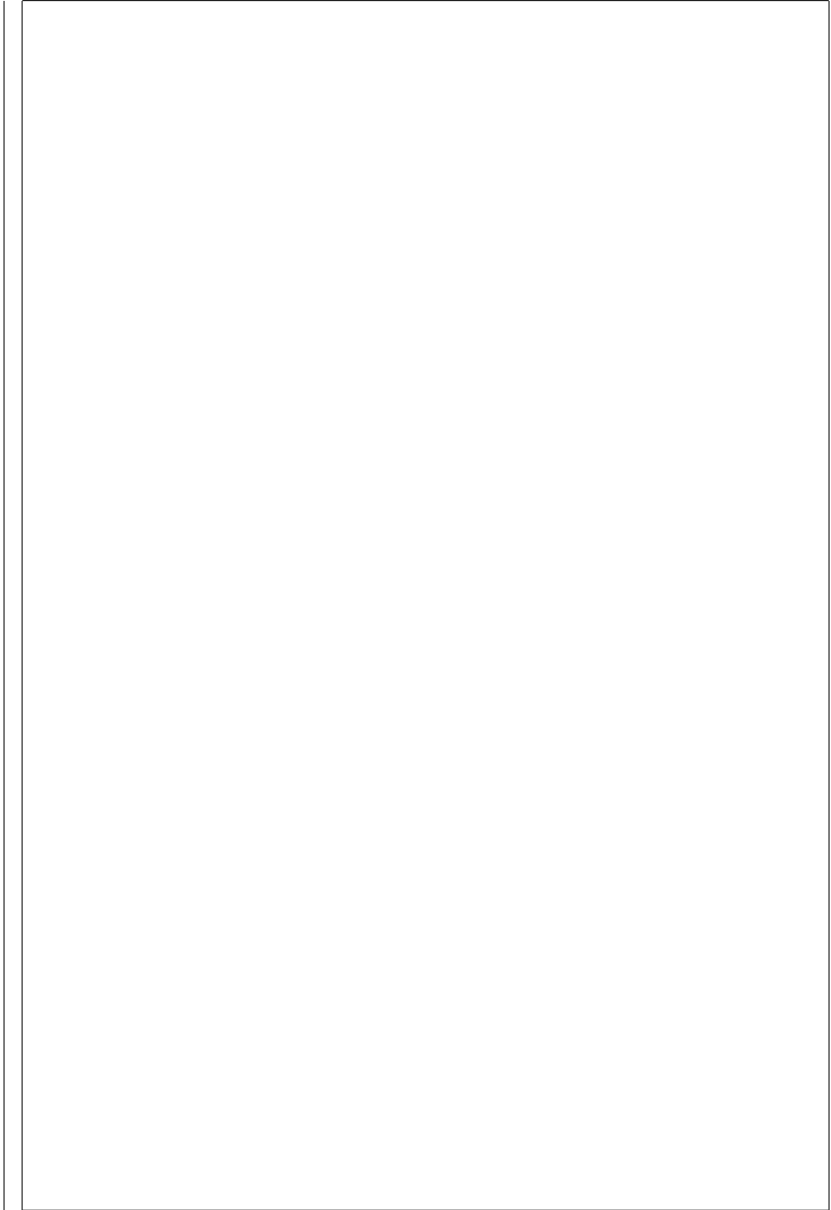
## Chapter 7

# Price in X

I don't care about the fiat price. Which of the x currencies to i value it in? Although so-called atomic conversions between fiat currencies are useful, and for the transition to a hyperbitcoinisation, their exchange rate is meaningless. I can have 1 BTC or USD EUR YEN GBP<sup>1</sup> LEBONASE, EGY, ..., 120 currencies. History has shown that the trend of all government-issued currencies is to 0 as time increases. So if this is indeed the winner, as I believe, why would you ever convert to any of the 100 existing government-controlled currencies. Saying that, it appears the number does indeed go up (NGU), with STF, power-law when fitted to the dominant fiat currency, the USD. Are we seeing Weinmar inflation against the dollar since Satoshi Nakamoto's discovery? If history doesn't repeat but rhymes, 4th turning and sovereign individual thesis are playing out, then yes. The USD, which all other currencies are pegged against, is undergoing hyperinflation as measured against bitcoin.

---

<sup>1</sup>BTC transaction volume as of 2024 has overtaken GBP, making it the 4th largest currency in final settlement.



---

---

# Chapter 8

## Adoption

### 8.1 Nation State Adoption

Creative way to express the evolving perception of Bitcoin in a humorous manner. In the Bitcoin community, there have been various perceptions and stereotypes associated with Bitcoin over the years. One humorous representation of this evolution is as follows:

2010 No one uses it

2012 Only computer nerds use it

2013 Only drug dealers use it

2014 Only money launders use it

2017 Only gamblers use it

2018 Only a small percentage of the population uses it

2020 Only small companies use it

2021 Only small countries use it

2024 Only small states use it



This representation humorously captures the changing perceptions and stereotypes surrounding Bitcoin over time.

El Salvador, translating from Spanish to English as “The Savior”.

<https://www.nobsbitcoin.com/bukele-reveals-el-salvadors-bitcoin-a>

## 8.2 CEOs

Michael Saylor saylor #Bitcoin days are numbered. It seems like just a matter of time before it suffers the same fate as online gambling.  
8:18 PM - Dec 18, 2013

Michael Saylor saylor #Bitcoin is a swarm of cyber hornets serving the goddess of wisdom, feeding on the fire of truth, exponentially growing ever smarter, faster, and stronger behind a wall of encrypted energy. 2:51 AM - Sep 19, 2020

how started vs how going

---

---

---

# Bibliography

Saifedean Ammous. *The Bitcoin Standard: The Decentralized Alternative to Central Banking*. Wiley Publishing, 1st edition, 2018. ISBN 1119473861.

Andreas M. Antonopoulos. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. O'Reilly Media, 2014.

J.D. Davidson and W. Rees-Mogg. *The Sovereign Individual: How to Survive and Thrive During the Collapse of the Welfare State*. Simon & Schuster, 1997. ISBN 9780684810072. URL <https://books.google.co.uk/books?id=04a0AAAAIAAJ>.

Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Bitcoin.org*, 2009. URL <https://bitcoin.org/bitcoin.pdf>.

George Orwell. *1984*. Tandem Library, centennial. edition, 1950. ISBN 0881030368. URL <http://www.amazon.de/1984-Signet-Classics-George-Orwell/dp/0881030368>.

Nick Szabo. Shelling out: The origins of money, 2002. URL <https://nakamotoinstitute.org/shelling-out>.