# Title: Decrypting Money

## Subtitle: A Comprehensive Introduction To Bitcoin

## Authors: Marco Krohn, Anthony Jefferies, Marco Streng, Zoran Balkic

### Contents:

Foreword by Garry Kasparov ….xi

Introduction… .XV

PART 1: THE HISTORY OF MONEY… 1

1. The Origins of Money …….3
2. The Functions and Properties of Money 29
3. The Digitalization of Money. …………47

PART 2: BITCOIN, THE FIRST CRYPTOCURRENCY 63 |

1. Bitcoin History 65
2. Bitcoin Structure. 99

PART 3: HOW BITCOIN WORKS. 131

1. Bitcoin Fundamentals.. 133
2. Cryptographic Primitives … 177
3. Bitcoin Mining… 203

Conclusion… 273

Chapter Notes:

### Foreword by Garry Kasparov ….xi

* THOUGHT EXPERIMENT: IMAGINE YOU ARE a dissident fighting for democracy in Venezuela.
  + Government monitors your every move, tracking what financial transactions you are allowed to make and chasing your footprints (both digital and physical) everywhere.
  + What can do? How can you survive and continue to speak out?
* A book like Decrypting Money to help us move into the phase.
* I’m also a natural skeptic, however, so his passion for the subject of cryptocurrency wasn’t enough to convince me. It was his desire to look beyond the hype of the moment, all the speculation and the to present coherent plans and prospects for “internet money” in the near and distant future. Myths, to present coherent plans and prospects for “internet money” in the near and distant future.
  + More important than cool tech and social buzz when goal is to change the world.
  + **Free speech in the internet age,** for example, along with data ownership, privacy, and cybersecurity.
    - Created endless possibilities, including new threats and exploits,
* Our tech is agnostic, neither good nor evil. It’s how we use it.
* I’m **not sure I’ll live to see it, although I hope I will**, because it will indicate that so many other positive transformations in **personal freedom and societal change**

### Introduction… .XV

* Figure 0.1: The first block of the bitcoin blockchain contains
* BOOK STEMS FROM OUR INDIVIDUAL stories of how we first encountered bitcoin.
* None of us could have imagined how life-changing bitcoin ſould be for us.
  + Between 2011 and 2013, we all separately and rather different ways were introduced to, learned about,
  + Marco had a PhD in theoretical physics, a job in the banking industry, and an opinion: The idea was crazy. It couldn’t work.
* TOWARD A DEEPER UNDERSTANDING
  + Bitcoin doesn’t have to be arcane, but books on the subject tend toward either the simplistic or the extremely technical.,
  + Mathematical and conceptual complexities separated our friends and too many other interested non-experts
    - **Founded Genesis Mining to bridge that gap. This book is an extension of that bridge.**
    - Neither an “Idiot’s Guide” nor a university-level text on cryptocurrencies
    - Interested, intelligent laypeople
  + 1 Bitcoin is both a currency and a payment system. Initial Using upper- and lowercase versions of the letter “B,” such that “bitcoin meant the currency (as in, “I owe two bitcoins”), while “Bitcoin” referred to the system itself
* BOTH PHILOSOPHY AND CURRENCY
  + Conversation on a cypherpunk mailing list out what a better form of money would look like, and its origin shaped
  + Place a high premium on protecting individual privacy.
    - **Privacy is not secrecy.** A private matter is something one doesn’t want the whole world to know, but a secret matter is something one doesn’t want anybody to know.
      * Privacy is power to selectively reveal oneself to the world.
  + 2 A white paper is an in-depth document that describes a specific topic.
  + 3 “Cypherpunk” is derived from the words “cipher” and “cyberpunk.”
  + 4 Eric Hughes, “A Cypherpunk’s Manifesto,” Activism.net, March 9, 1993
  + Figure 0.2: Bitcoin supply curve
* ABOUT US
  + Degrees in mathematics and engineering, as well as a in computational fluid dynamics, Anthony Jefferies
    - Relevant concepts arrived at bitcoin, such as public-key cryptography and distributed computing.
    - Development of quantitative tools bitcoin data analysis. Simulations for the research and development division.
  + Each of us had our own “down the rabbit hole” moment,
    - Enthusiastic about the possibilities it
    - Simply the next logical step in the evolution of money.

### PART 1: THE HISTORY OF MONEY… 1

### The Origins of Money …….3

* Examples of the very diverse types of money that humankind invented
* Learn about its properties, and also many cases why a currency eventually failed.
  + People seem to have a vague fore we worked meta
  + Intuitive view promulgated (without evidence) by the ot of Nations.
  + Little ethnographic evidence that a barter economy ever existed, much less evolved into currency-based
    - Money seems to have been an abstraction from the beginning, and its history is full of austraction
* 1. COMMODITY MONEY
  + Perhaps the least abstract form of currency, commodity money is itself useful and of intrinsic value.
  + 1.i. Cowry Shells
    - Organic intricacy renders it difficult counterfeit, while its uniformity of size makes it possible to assess multiples bY weight, eliminating the time-consuming of counting each individua
  + 1.ii Rai Stones
    - heavy)
    - Rarely changed physical location) but by declaration.
      * Continued to be treated as usable currency when it sank to the bottom of the ocean on
    - David Dean O’Keefe was shipwrecked on the **introducing iron tools and large sailing vessels**, which dramatically increased the speed at which the rai stones could carved and transported.
  + 1.iii. Roman Denarii
    - Formalization replaced the use of coins of various sizes compositions whose value had been exclusively determined by weight.
    - 13 Debasement is the reduction of the silver content of a coin, for example, by educing its weight or purity.
      * Gresham’s Law:
        + Principle that “bad money Drives out good money
  + 1.v. Cigarette Money
    - In POW camps and prisons,
* 2. REPRESENTATIVE MONEY
  + (Usually paper) to represent some form of commodity money (usually coins/precious metals).
    - The US dollar, for example, was representative of the gold for which it could be nominally redeemed until the 1970s.
  + 2.i. Paper Money
    - the first government-backed paper currency> the Jiaizu - China 960
      * First paper currency to experience the inflation 1d-reform ycle
  + 2.ii. The British Pound
    - Lose 99 percent of its purchasing power luring the twentieth century.
    - Bretton Woods System, the pound and many other world -currencies were linked to the US dollar, which was at that point still backed by gold.
  + 2.iit. Three New Issues
    - The Double-Spend Problem
      * Check fraud,
    - Fractional Reserve Banking
      * If everyone who trusted the goldsmith to store their gold for them tried to collect it on the same day, there wouldn’t be enough to cover the receipts of deposits
    - Bank Runs
      * Ers attempt to withdraw their deposits because they are worried about the bank’s solvency.
        + Cause a feedback loop in which customers become more anxious and make more withdrawals until the system collapses.
* 3. FIAT MONEY
  + From the Latin word meaning “let it be done,”
  + Made legal tender by government decree (fiat) and derives its value from that decree 2
* 4. MONEY AND THE STATE
  + Historically, nation-states have claimed the exclusives right issue currency.
    - The interests of the state and the people are not necessarily the same, the **government does not always act in the interest of the people.**
  + 4.i.Central Banks
    - Federal Reserve in the United States, the European Central of the Eurozone, and the Bank of Japan and People’s of China
    - International Monetary Fund (IMF), whic
      * Coordinates between national financial stems
  + 4.ii, Private Money
    - Between 1837 and 1866, the federal government no regulations on who was entitled to issue currencies.
    - Churches, banks, and railroad companies-all devised, printed,
    - Eight thousand different currencies in use
    - Airline frequent flier miles, although
  + 4 iii. Free Banking
    - If banknotes issued by one bank were deposited at another bank, they would be accepted that bank, and would be returned via a clearing mechanism the original bank.
    - Practice incentivized cautious decision-making reduced the chances that one institution could damage reduced the chan
    - Hayek has argued such a free-banking system would liberate not only banks but their customers.
* CHAPTER SUMMARY
  + Commodity money must physically present to be exchanged.
    - Representative money solved this issue while introducing new ones-the double-spend problem and fractional reserve banking with its risk of bank runs.
  + Gave the governments that issue and regulate them more control over the amount of money and debt available.
  + Relative strengths and weaknesses of such a diverse field and to consider how the next stage of money’s evolution
  + well-designed traits that would make it an excellent form of money.

### The Functions and Properties of Money 29

* If money had no physical form, was it money ?
  + Integral parts of our everyday lives are interesting in and of themselves.
* 1. THREE FUNCTIONS OF MONEY
  + 1.i. A Medium of Exchange
    - An intermediary instrument, which may not necessarily be useful for the person possessing it, used to Facilitate trade by serving as an agreed-upon standard of value.
  + 1.ii. A Unit of Account
    - An apple in city is worth more than it is on the farm and less in late summer when it’s in season than in winter when it’s had to :» preserved. Ability to measure value also unifies an economy
    - Compare the value of different goods and services.
  + 1.iii. A Store of Value
* 2. TRAITS OF MONEY
  + 2.i. Scarcity
    - Because money is used to represent the value of these resources, money itself must be carce.
    - Currency decouples from precious metals
    - The Superdollar
      * Introduction of the 3D security ribbon as well as aggressive international forensic action.
  + 2.ii. Durability
  + 2.iii. Portability
  + 2.iv. Divisibility
  + 2.v. Fungibility
    - Perhaps the least obvious and intuitive of the raits of money, is the one that enables a unit of a currency to be interchangeable
    - Gold is fungible and rubies aren’t,
    - The more fungible a currency the better it can perform its functions as a unit of account, a medium of exchange.
  + 2.vi. Security and Countriting
    - Resistance to counterfeiting is | important in establishing this confidence. Holographic images, foil components, transparent features, micro letters, and raised ink. Ultraviolet lights, detector pens,
    - Figure 2.1: Traits of money source: W. Stanley Jevons, Money the Mechanism of Exchange York: D. Appleton and Company, 1877], 30-40.)
* 3.ASSESSING MONEY BY FUNCTIONS TRAITS
  + 3.vi. Comparison of Different Currencies
    - Figure 2.2: Comparison of the traits of cowry shells, rai stones, gold, diamonds, and fiat money
* 4. PAYMENT SYSTEMS
  + Evaluated by three significant attributes:
    - Security, Convenience, Mediation.
      * Create illegitimate
      * How easy it stows
      * Involvement of a third party
      * Improving security makes the system harder to use.
    - Peer-to-peer transactions: transactions done directly, one arson to another (without intermediary),
    - Electronic systems are more secure and convenient for most
  + Figure 2.3: Comparison of payment systems
* CHAPTER SUMMARY
  + Practically every human society invents some kind of money”
    - Certain fundamental needs,
    - Physical realm and into the digital one.
    - Bitcoin Was the first,

### The Digitalization of Money. …………47

* The idea of money becomes most closely connected to a number
* Figure 3.1: The US money supply (Board of Governors o th Federal Reserve System [US], M2, Fral Rsrv Bank o St.
* Abstraction o a symbol or representation has become so obscure as to be practically impenetrable. Grounding in what money is, it’s time to take that step
* 1. DIGITAL PAYMENT SYSTEMS
  + The telegraph, capitalizing on advances in our understanding electricity, radically increased the speed and efficiency of communication.
    - Nearly real-time reliable communication
    - Starts of Morse code,
    - Stops and starts of Morse code,
    - Speed at which such transactions be tabulated
  + 1955, Bank of America gained a significant competitive lvantage by moving from an electromechanical method of ministering bank accounts anc check-handling systems to electronic one using
    - Range of more convenient locations and at more flexible hours
* 2. DIGITAL FIAT CURRENCIES
* 3. DIGITAL PRIVATE CURRENCIES
  + 3.i. E-Gold
  + 3ii. Liberty Dollar
  + 3.iii. Linden Dollar
    - Purely virtual currencies that preceded bitcoin, the Linden dollar operates in the virtual world of Second Life essentially
  + 3.iv. DigiCash
    - Y too few enrolled, and fell victim to what Chaum called the “chicken/egg problem.”
    - few customers wanted to make purchases with DigiCash to motivate merchants to try it out, and too few merchants accepted it to motivate customers to use it.
  + 3.v. B-Money
    - Not advance beyond set of documents written in the 1990s bY computer engineer Wei Dai.
  + 3.v1. Bitgold
    - Recognizing that computational power was likelY to increase, which would make a digital currency progressively easier to create, thus driving inflation, Szabo included timestamping on the prem- ise that the value of any individual unit of Bitgold would be tied the time it was created.
  + 3.vii. Hashcash
    - For legitimate users, this fee would be vanishingly small, but for spammers sending millions of emails it would be, if not prohibitive, at least a deterrent.
    - Concept of a proof of computational work
* 4. CRYPTOCURRENCIES AND BITCOIN
  + Cryptography is itself a portmanteau derived from Greek words kryptos (meaning “hidden” or “secret”) and graphein (“writing”).
    - Decentralized control system
* CHAPTER SUMMARY
  + First non-state, math-backed digital currency to survive its infancy.

### PART 2: BITCOIN, THE FIRST CRYPTOCURRENCY 63 |

### Bitcoin History 65

* 1. SATOSHI NAKAMOTO
  + 1.i. His Identity
    - The cypherpunk mailing list:39
  + 1.ii. His Genius
    - Cryptographic primitives are well-established, low-level cryptographic algorithms that are frequently used to build cryptographic protocols for computer security systems. 41
      * He didn’t invent any new cryptographic functions, but took the hashing algorithm from Hashcash distributed ledger of B-money, and the cryptographic secuthat Digicash used.
      * Newer isn’t better. Newly invented components haven’t been tested enough to be trustworthy.
    - Double-spending
      * Twas a well-known issue within the computer science community.
  + 1.iii. His Agenda
    - Laid out a set of well-defined design goals for the new digital currency in his white paper and discussed many of them the cryptography mailing list.
  + Decentralized .
    - Recognizing that every centralized system is, ultimately, based trust, Satoshi believed in the importance of decentralized© -
    - Individual participants rely only on themselves and are solely responsible for the security of their accounts, system can have no single point of control on which it depends.
      * Distributed control wasn’t a new idea. The internet itself is decentralized.
        + Outgrowth of a Defense Advanced Research Projects Agency (DARPA) project called ARPANET (Advanced Research Projects Agency Network)
        + developed in the 1950s under threat of nuclear attack
    - Napster
  + Peer-to-Peer
    - Society for Worldwide Interbank Financial Telecommunication (SWIFT): an international system using standardized message syntax to communicate money transfers between inks.
  + Software Updates on the Bitcoin Protocol
    - Organizations can be compelled to update software in order to continue to us it.
    - Set of rules accepted by compatible clients
  + Pseudonymity
  + Open Development
    - Other people can check the code, and, if there are mistakes in the codebase (often referred to as “bugs»), the chances are higher that someone will eventually them.
    - build trust in the system,
    - People studying the code find improvements or approach recruits additional highly skilled) developers who contribute to the code.
  + Scarce
    - Any system that assumed the risk of refunding purchases would be motivated to vet the vendors to whom it sent payments and to investigate both the identity and legitimacy of people requesting refunds.
  + Minimized Feature Set
    - leanness in bitcoin’s programming ɔntributes to the stability of the network while still allowing participants to do more complex things than simple A to B transactions
* 2. BITCOIN’S RECEPTION
  + 2.i. The White Paper
    - November 2008 it TITON not an overnight sensation.
      * Reaction was a lukewarm “Yeah, that’s kind of cool,” and Satoshi had some trouble convincing anyone try out the first version.
      * Nearly died in its first Year from lack of interest.
    - Genesis block: the name of the first block of a blockchain
  + 2.ii. Early Valuations
    - That point, approximately 0.0025 US cents. Until
    - Only theoretical constructs
    - Became easier to purchase and sell bitcoins
    - Figure 4.6: Bitcoin price over time (note the logarithmic scale of the USD price)
      * Increase was not smooth, but exhibited some very fast surges and dips in the first few years.
  + 2.iii. Volatility
    - In the early days, bitcoin’s price didn’t correlate strongly with traditional assets as reflected in the various stock markets.
    - Buy and trade it primarily as a store of value,
  + 2.iv. Early Participants
    - They were playing a “Let’s see what happens if” game.
    - Gavin Andresen Bitcoin Faucet 48
  + 2.v. Mainstream Attention
    - Bitcoin and Governments
    - Market capitalization (often referred to as “market cap”)
    - Figure 4.8: The above map shows the legal status of bitcoin worldwide as of 2022
    - Financial Institutions
      * Banking operating procedures and IT takes a lot of and effort.
        + Obliged to verify the identity
        + Able to reverse a transaction,
        + Held by known natural or legal persons,
        + Regulated by national financial regulators,
        + Secure and specialized protection system.
      * Relatively small market size of bitcoin, banks did not that integrating bitcoin was worth the effort.
      * Know Your Customer (KYC): a process that obliges most banks and insurance companies to check who their customer and where their funds originate from.
      * Anti-Money Laundering (AML): a set of controls and procedures primarily adapted by financial institutions to prevent, detect report money-laundering activities.
  + 2.Vi. Cryptocurrency Ecosystem
    - Competitors started to pop up everywhere.
    - Minor projects copied, others were released that were completely written from scratch.
    - Ethereum was released in July 2015
* CHAPTER SUMMARY
  + Identity remains uncertain and obscure, Satoshi akamoto’s genius is self-evident and incontestable.
  + Entirely new form of money.
  + Abstraction whose utility makes it ubiquitous throughout human civilization across cultures,
  + Deliberately, in service to ideals grounded in a belief money, a foundational economic good, could be better.
  + Payment system that is decentralized to protect against single points of failure.
  + Mathematics rather than government fiat.

### Bitcoin Structure. 99

* Better understand bitcoin’s strengths and advantages, as well its issues, we should explore its structure and examine performs as both a currency and a payment system.
* 1. BITCOIN CURRENCY
  + 1.i. Scarcity and Security
  + 1.ii. Divisibility
    - Satoshi: the smallest division (one one-hundred-millionth) of bitcoin.
  + 1.iii. Durability |
    - Private Key: an alphanumeric fifty-two-character string, similar to a password, needed to transfer bitcoin.
  + 1.iv. Portability
  + 1.v. Fungibility
  + 1.vi. Comparison of Traits
    - Figure 5.1: Comparison of traits of bitcoin, fiat currency, and gold
    - Bitcoin’s underlying traits make it an excellent form of money.
* 2. THE BITCOIN PAYMENT SYSTEM
  + 2.i. Decentralized and Peer-to-Peer
    - Individual payment systems itself, centralized. The government could shut any of them down as easily as it did Napster
  + 2.ii. Transactable
  + 2.iii. Secure
  + 2.iv. Open Protocol and Open Source
  + 2.v. Public Ledger
    - Weighs nothing at all and leaves little to memory:
* 3. PROPERTIES OF BITCOIN
  + 3.i. Uptime
  + 3.11. Transaction Fees
    - The higher the man or transaction validation, the higher than average fee
  + 3.iii. Stability
    - Bitcoin motto vires in numeris (strength in numbers)!
  + 3.iv. Pseudonymity
    - Figure 5.2: Comparison of degree of privacy of bitcoin and cash
    - A bitcoin address or bitcoin account is an alphanumeric identifier for an account that holds bitcoin
    - Figure 5.3: Alice’s bitcoin wallet transfers 6.0 BTC to Bob’s wallet.
    - Mix of transparency and privacy, with a public transaction ledger but Pseudonymous account holders.
* 4. ISSUES WITH BITCOIN
  + Human and technical
    - Risks associated with bitcoin potentially pose a threat the network. Drawbacks are more subjective.
    - A degree of anxiety. Over the long term, such nervousness tends to diminish as experience holding bitcoin develops.
  + 4.i. Possibility of Errors
    - Possible-even probable-that its code is somewhat less than flawless.
    - Reverting back to the older version.
    - Limits still need to be explored, and there may be bugs or shortcomings that have yet been discovered. However, it’s done remarkably well for over a decade.
  + 4.ii. Technical Risks
    - Risk of Fracturing through Community Dispute
      * Result in two branches: one that follows the original protocol, and one that follows the
      * A (hard) fork is a split of the bitcoin network resulting from participants following different protocols.
    - Conservative Development Approach
    - High Energy Usage
      * Many of the people who’d need to gree to such a shift are heavily invested in existing machines despite their electricity cost. It’s hard to imagine them voting against their own int
  + 4 .iii. Abuse
    - Attacker that controls 51 percent of the mining hardware would have the possibility to disturb the network, e.g.,
      * Intentionally excluding transactions (censorship.
      * By modifying the order transactions,
      * Or by reversing transactions.
      * Attacker would not be able to steal bitcoin from user wallets.
  + 4.iv. Illegal Content
  + 4.v. Lack of Appeal
  + 4.vi. Fractional Reserve Banking
  + 4.vii. Reputational Issues
    - With the possible exception of public inion, none of this had a lasting negative impact on bitcoin.
  + 4.viii. Possibility of Government Interference
  + CHAPTER SUMMARY
    - Outperforms its predecessors on all these metrics.
    - An engineered rather than evolved system, bitcoin adds most perfect uptime; equitable, market-driven transaction political and economic security; and pseudonymity to its list of advantages.
    - Are risks and drawbacks to bitcoin,
      * Remarkably few serious setbacks

### PART 3: HOW BITCOIN WORKS. 131

### Bitcoin Fundamentals.. 133

* 1. TERMINOLOGY
  + 1.i. On Bitcoin Addresses and Private Keys
    - This collection of characters is called base58. Usually, you would expect possible. This collection of characters is called base58. Usually, you would expect be used; however, as the characters O, O, “I” (small “L”), and “I” (capital “i”) in some used; however, as the characters 0, O, “I” (small “L”), and “I” (capital “r”)
    - 61 This view is a bit bitcoin internally does simpaned not have ναι பப tips in understanding the vas only take transaction outputs and track hether these are “spent” or “unspent” (cf. Chapter 6.2.iii)
    - The reason is that the address space is so large that Alice and Bob would (almost certainly) not generate the same address even if they both generated addresses nonstop on supercomputers for millions of years.
    - Term “bit” is a combination of the words “binary” and “digit.” he name was invented by John W. Tukey. Private keys start with a “5” (which is purely a convention to make them easily recognizable).
  + 1.ii. The Bitcoin Ledger
    - Figure 6.1: A traditional ledger
    - A “bitcoin node”) stores a copy of the list of bitcoin addresses, and the number of bitcoins stored at each address.
    - Held and maintained by thousands of machines worldwide, thus decentralizing the system extremely effectively and contributing to its robustness.
    - A public ledger that keeps records of all account balances and transactions,
    - Distributed to thousands of computers (also referred “nodes”)
    - Only showing account addresses, not the names of owners (“pseudonymity”).
  + 1.iii Bitcoin Transactions
    - Is irreversible.
    - There is no equivalent of the bank for Alice to contact, and no possibility for her to reverse the transaction, other than asking Bob to send the Bitcoin back.
* 2. BITCOIN MANAGEMENT
  + 2.i. Bitcoin Wallet
    - A program or service that stores and manages a collection of bitcoin addresses that belong to same user.
  + 2.ii. The Change Address
    - Send the remainder of the funds to that address. All this happens under the hood and most users will not even notice it.
    - Besides privacy concerns, there is another reason for not reusa bitcoin address: the security of a bitcoin address that was already used is slightly weaker, though still reasonably strong For most purposes,65
  + 2.iii. Accounts and UTXOS
  + 2.iv. Tainted Coins
    - Coins with a “questionable” history are sometimes referred to as “tainted coins.”
    - Distinctions between different bitcoins, there are potential consequences for bitcoin’s fungibility trait (cf. Chapter 2.2.v), as pure fungibility would imply absolutely no difference 2.2.V),as pure
  + 2.V. Hierarchical Deterministic Wallet
    - Or HD Wallet
    - Implemented to make this process more structured and orderly.
    - Instead of generating individual private keys separately, first welve (or twenty-four) words (called seed words or seed) chosen from a list of words in a standardized 2048-word dictionary.
    - Physically on paper or in metal form so they can be secured are safe from computer hacking, as they are not stored electronically
* 3. TYPES OF WALLETS
  + 3.i. Paper and Metal Wallets
  + 3.ii. Hardware Wallets
  + 3.iii. Software Wallet on Computer (Online/Offline)
  + 3.iv. Mobile Phone Wallet
  + 3.v. Online Wallet
  + 3.vi. Brain Wallets 請
  + 3.vii. Summary
    - Figure 6.11: Comparison of the security of bitcoin wallets
      * Access to the hardware device occurs via a USB cable. While there is no air-gap between the computer and the hardwallet, we are also not aware of any security issues with USB connection, and thus consider hardware wallets to ‘cold.”
* 4. ACQUIRING BITCOIN
  + 4.i. Cryptocurrency Exchanges
    - Security
      * Two factor authentication (“2FA”) is one frequently used security measure at
  + 4.ii. Other Means of Acquiring Bitcoin
    - Bitcoin ATM
    - In Person
* 5. MINING AND ACHIEVING CONSENSUS
  + A set of rules and procedures that leads to consensus is referred to as a consensus algorithm or consensus mechanism.
  + 5.i. Transaction Processing in a Centralized System
  + 5.ii. Achieving Consensus in a Decentralized System Is Difficult
    - Most transactions will normally be carried out by honest actors an b unisput. If all transactions were like that, the system would be sufficient.
      * It must maintain its integrity if two contradictory transactions are sent to the system.
      * The double-spend problem can be solved, because the central authority can order events in time (this is called time-ordering). It
        + Different nodes will hear about the existence of the Bob and Charlie transactions at different times. Some
  + 5.iii. Blocks and Bitcoin Mining
    - Miners or mining nodes) that is vital for eaching consensus. In
    - Bitcoin transactions are bundled together in groups that are called blocks. These blocks are an important part of a structure called the blockchain, which
    - Many different terms are used to describe the process of selecting transactions, forming a block, and solving the complicated mathematical problem:
      * Creating, producing, solving, finding, and mining a block are all used synonymously.
    - The new bitcoins generated as part of the new block (also called the block reward). This
      * Only way that new bitcoins are created.
    - Second component is through transaction
    - Solved a block or mined a block or produced a block.
  + 5.iv. The Bitcoin Node Network
    - Designed to be decentralized and peer to-peer, where everyone can take a part in it without anyone’s permission (this property is also referred to as permissionless).
    - Each node will independently verify all transactions and blocks it receives; are gatekeepers that filter out malicious transactions and locks (e.g., double-spending attempts).
    - A bitcoin node usually refers to a full node,
      * A complete history of all blocks
      * Download all blocks (beginning with the first block) its peers.
      * Will validate all blocks and transactions, beginning the very first
      * It checks and relays unconfirmed transactions to other checks and
      * It will share its copy of blocks to other nodes if requested.
    - A mining node, a node that can produce a new block, must be a full node. Othe
    - Property of withstanding even major damage (like a loss of a number of nodes) is referred to as resilience.
    - Freely downloaded and used without any restrictions.
    - Backbone of the infrastructure for bitcoin wallet clients and miners.
* CHAPTER SUMMARY
  + Status of all transactions is tracked by the global bitcoin ledger, copy of which is stored on every node.
  + Remain in agreement in bitcoin’s decentralized system is an energy- and cost-intensive system called mining, which gathers a number of transactions together into a structure referred to as a block.

### Cryptographic Primitives … 177

* IN THE 1999 FILM THE MATRIX, NEO WAKES UP TO HIS COMPUTER directing him to: “Follow the white rabbit.” He does and ends
  + Bitcoin rabbit hole goes very deep.
  + Shifting metaphorical gears, if we’re driving, not diving, the previous chapter provided what we hope is a useful driving manual while the ones before it explained how and why a car operates the way it does.
    - Better understand its operation, this disassembles the vehicle.
  + Cryptographic primitives are well-established, elementary cryptographic algorithms that are often used in cryptographic protocols
* 1. CRYPTOGRAPHIC HASH FUNCTIONS
  + Bit like fingerprint-making machines. They produce a compact identifier (called a digest or hash) whose relationship to input data is like that of fingerprint to person.
    - Complex mathematics of hash functions is **beyond the scope** 
      * Best thought of as black boxes that accept inputs and produce outputs.
  + 4 .i. Properties
    - Important to bitcoin being SHA-2.70 (SHA stands for Secure Hashing Algorithm.)
      * In bitcoin literature, there are also often references to SHA-256; for all intents and purposes, these are the same.
      * Probability of finding a collision among a billion hashes is 1 in 4.3 x 10-60, and it is orders of magnitude less likely than the being hit by a “killer” asteroid.
    - They are deterministic.
    - Small changes in the input cause huge change in the ‘avalanche effect”).
    - They are generally quick to compute.
    - They are unidirectional.
    - The output always has the same
  + 1.ii. Applications
    - Password Storage
    - Bitcoin Addresses and Fingerprints
      * The last four bytes (=8 characters) are referred to as the fingerprint, and adding those reduces the chance of mistyping a address to about one in four billion.
* 2. PUBLIC-KEY CRYPTOGRAPHY
  + 2.i. Secure Communication
    - Public-key cryptography (or asymmetric cryptography) was developed more than fifty years ago, and it been proven to withstand all attempts to break it,»
  + 2.ii. Proof of Ownership
* 3. DIGITAL SIGNATURES
  + 3.1. Single Signatures
  + 3.ii. Public-Ky Cryptography Bitcoin
  + 3.iii. Signing Bitcoin Transactions
  + 3.iv. Multiple Signatures
* CHAPTER SUMMARY
  + Smallest change in that information produces a radically different ha sh, same data always generates the same hash-a
  + Primitives were then combined to construct a method of digital signatures, which like traditional signatures can be used to verify both the contents of a message and that the sender is genuine.

### Bitcoin Mining… 203

* Bitcoins are less unearthed than created the moment the first miner solves a block’s riddle, which is called solving the block.” This alchemical process has two steps:
  + building a (candidate) block and solving it.
* 1. BUILDING A CANDIDATE BLOCK +r
  + - As-yet unconfirmed requests that have propagated through the network. From this pool, miners select which transactions to verify. So
  + 1.i. Transaction Selection
    - * A typical size of a bitcoin transaction is around 250 to 500 bytes.
      * Transaction data is limited to 1 MB. However, additional data MB. However, additional data related to digital signatures can, for certain transaction types, be stored outside of structure (up to 3 MB), resulting in an “effective block size” limit of 4 MB (1 MB transaction data + 3 MB signature data). ir
    - Figure 8.1: Three possibilities how inputs and outputs can be combined
    - Miners usually optimize for the highest fee-per-byte.
  + 1.ii. The Candidate Block
    - Rules of block format prohibit the inclusion of two transactions that “spend” same bitcoin (the so-called “double spend” that we disce\_a ssid
      * Including one of the two transactions in a block is perfectly fine, but including both of them would be a violation of the rules.
      * Only after the mathematical puzzle is solved a candidate block become a “real” block, which then i s published.
    - Figure 8.3: From the unconfirmed transaction pool to the bitcoin node network
  + 1.iii. Coinbase Transaction
    - A block cannot be completely empty. At minimum it must hold at least one transaction. The first, and the mandatory, transaction is called the coinbase transaction, This is the transaction with the bitcoins that a miner earns for successfully solving a block, and has the following two components:
      * Newly created bitcoins (th block reward”)
      * 2. The transaction fees
        + Cannot be spent until an additional 99 blocks have been thereafter,
        + A few additional blocks, one fork will prevail while the other one will be discarded (including all its coinbase transactions),
        + Ensures that all bitcoins are equally trustworthy.
  + 1.iv. The Block Header
    - The Merkle Root
      * Data structure is used to organize the hashes all transactions in a block called a “Merkle tree”
        + The “Merkle root,” which is calculated using the data in a Merkle

If a transaction in the block is changed, this will invariably also change the Merkle root

* + - Timestamp
      * For adjustment to the difficulty
        + The “no earlier than” rule: the time entered by the miner must be later than the median timestamps of past eleven blocks that were added to the ledger
        + The “not too far in the future” rule: more than two hours ahead.
    - Hash of the Previous Block
      * Linking the blocks together 84
        + Only the hash of the block header (and not of the block itself)
* 2. BUILDING A BLOCK
  + New blocks that are circulated between participating nodes will be checked by each node individually
    - Whether the block and its transactions meet all the requirements.
    - Mantra of “don’t trust, verify,” meaning that nodes do not trust each other, but verify everything on their own.
  + 2.i. Too Many Blocks
    - Process of creating a valid block is deliberately slowed down
  + 2.ii. Bitcoin’s Mathematical Problem
    - SHA-2 (block-header) ≤ Target Hash (Equation 1)
      * 85 In reality, bitcoin applies the SHA-2 hash function twice, i.e., SHA-2(SHA-2(blockheader)) is calculated on the left hand side
    - Target hash (often only called the target). The target is chosen to slow down the block production
    - 80 byte block header) and return a big integer number (the tput value is between 0 and - 1.15 × 107).
      * Try again repeatedly with different block hars “nonce”
      * The value is an arbitrary number used only once, and purpose is to alter the block header such that the above condition can be satisfied.
    - ‘Deterministic” property of the hash function, miner has to change the nonce if the previous attempt was
    - Because of the “avalanche effect” there is no benefit of knowing that the last attempt was already “close”
    - As A one-way function, it is not possible to take a hash that satisfies the condition and reverse the function to find a successful nonce.
    - Different mining nodes that start with the same also will not do the same work twice
      * Have their own address to receive the block reward
  + 2. Iii. Hashrate
    - Primary determinant of success is the ability to test as many nonce values as quickly as possible.
    - Attempts-made (hashes)-per-second, also referred to as the hashrate an written as H/s
      * 1 terahash=1TH/s =1,000,000,000,000 H/s |
      * 1 Petahash =1PH/s =1,000,000,000,000,000 H/s
        + Modern mining machine (like Bitmain’s $19) calculate a hundred terahashes or a hundred trillion hashes per second.
        + Hundreds of thousands of miners across the world an average of ten minutes at this speed to solve one block!
  + 2.iv. Proof of Work
    - Repeatedly testing numbers against the threshold is energy- and time-intensive by design.
    - Verification must be exponentially easier to do than the verification
    - Military metaphor.
  + 2v. Target Hash and Difficulty Adjustments
    - E.,each node must independently be able to adjust the difficulty
    - No one exactly knows the hashrate of all participating
    - The average u should take exactly two weeks to m 016 blocks (=14 × 24 × 6).
    - New Target = old target × (time for the last 2,016 blocks weeks
    - As all nodes use the same timestamp, they will all independently come up with the same number for the new target hash.
* 3. BLOCKCHAIN AND CONSENSUS
  + - Self-regulated
    - Rule of the longest chain.
  + 3.i. The Blockchain
    - Transaction history.
    - Genesis block - first block
      * Modifying any block in the blockchain would mean that all succeeding blocks would immediately become id.
    - Immutability means the property that the contents of the lockchain are next to impossible to modify
      * Tamper-proof tamper-resistant.
    - Becomes more and more difficult to manipulate
  + 3.ii. The Longest Chain Rule
    - Two (or more) blocks link to the previous block is called a **chain split**. Let’s support
    - Nakamoto Consensus
      * stipulates that all nodes accept the longest chain as the version of the blockchain.
      * Agree on the same blockchain (and thus the me transaction history).
      * Vanishingly unlikely that competing chains persist for long.
        + Twice in a row is 2% × 2% = 0.04%, and so on

93 Although, research suggests it is much lower (Aat de Kwaasteniet, “Miners, Block Althougn, TEST] suggests it is much lower (Aat de

* + - Not benefiting from mining on an orphaned block is a strong incentive for miners to immediately switch to the longest chain
      * Stale blocks
      * Reoganization
        + Node receives a new chain with more cumulative computational work than the one it currently has, it discards blocks that are not in the new chain, and replaces them with the blocks in the new chain
  + 3.iii. Confirmations
    - Once a transaction is in the latest block, it is said to have one confirmation. Each block subsequently attached, it ceives an additional confirmation.
    - Figure 8.16: Confirmations and the blockchain
    - In theory (see Section 3.ii) no transaction is absolutely final, but after six confirmations, the probability that the network will reverse this transaction is nishingly small.
  + 3.iv. The 51 Percent Attack
    - What happens if not all miners are honest? In this
    - Is it possible for Mallory to produce more blocks than the honest nodes? Theoretically Yes.
      * Double-spend transactions
      * Prevent other miners from mining any valid blocks
      * Prevent transactions from going consequenc
      * An attacker can’t:
        + Create additional bitcoins Cexcept for the block ward), or send coins that never belonged to them.
    - Is Bitcoin at Risk?
      * 1. Building mining infrastructure on such a scale Is extremely expensi
      * One-off economic benefit.
        + Double Spend
        + Short price - to profit off decline in market price due to loss of confidence once detected
      * Mining honestly is economically more attractive.
        + Like stealing paper money by setting it on fire.
      * GHash.io briefly reached more than 51 percent of the overhashrate. While GHash.io did not have bad intentions, it raised major concerns within the bitcoin community. In the Ghash.io voluntarily promised to not exceed 40 percent
        + By 2015 GHash.io fell below 2 percent
      * Things already start to dangerous if an attacker has 30-40 percent of the overall hashrate
        + Controlling 40 percent of the total hashing the chances that a miner can double by mining six blocks faster than the other miners is 25 percent.
        + At 30% Selfish Mining strategy

Can compel other miners to follow

* + - Potential gain is comparatively small. So forthe same reaso we discussed before, a rational miner will always decide to be honest
  + 3.v. Summary
    - As of June 2021, bitcoin in its more than decade-long histo xf has never suffered a successful attack, and we believe it is now robust enough that this will not occur.
* 4. THE ECONOMICS OF MINING
  + - Guardians of the bitcoin network: they protect network and ensure consensus.
      * Do not this out of altruistic motives, but because they are profit-seeking participants.
      * The best economic interests of the niners are also in the best interest of the network.
  + 4.i. Mining Income
    - Dining Income = Block Rewards + Transaction Fees
    - Block Rewards
      * Average blocks are found every ten minutes, which is equivalent to 144 blocks per day,
        + or 7200 bitcoins that were produced every day during the first epoch (50 bitcoin per block)
      * The “block halving” event.
        + Every 210,000 blocks (approximately four years) the block reward halves.
        + Figure 8,19: Halvings of the block reward
    - Transaction Fees
      * Incentivized to select the transactions that generate the highit fee income for them ( can change ignificantly” time
        + Figure 8,22: Total transaction fees
      * Long-Term Considerations Until mid-2016 transaction fees were only responsible for about 1 percent of a miner’s income.
        + In 2021, number increased to about 5-10 percent, so
        + Fees indeed are becoming more important over time,
        + “Tragedy of the commons”: everyone would like to use a secure network, but noone is willing to (voluntarily) pay for it.
        + Bitcoin ensure a minimum level of transaction s by limiting the block size
  + 4.ii. The Network Hashrate
    - The sum of the hashrate of all machines
    - Estimating the Network Hashrate
      * No one knows its exact value
      * Can directly measure how many hashes per second their machines try out but not how many other niners have attempted in the same period.
      * Know how many mining machines are in use, where these 1ining machines are located, or whom they belong to.
      * The difficulty D is precisely defined, universal for all bitcoin nodes, and constant for roughly two weeks.
        + H=Dx2^32/600
    - Change as miners add or remove machines
      * For a period of time shorter than two weeks need to consider the current block production rate,
      * Less accurate estimates of hashrate.
    - The Hashrate Explosion (2009-2020)
      * Increased more than a trillion-fold
    - Mining “Satoshi Style” (2009-2010)
      * Home computers with a normal “central processing unit” CPU”).
      * “First generation of bitcoin miners’
    - GPUs for the Win (2010-2013)
      * In May 2010, Laszlo Hanyecz (the same person who bought pizzas for 10000 bitcoins)
        + Published an algorithm that allows using a “graphics processing unit” (“GPU”) mining bitcoin.
        + Hundreds of tasks in parallel - about one hundred times faster than a normal CPU (using approximately the same amount of electricity).

The “second generation of miners.”

* + - “The Rise of the (ASIC) Machines (2013-2014)
      * The first ASIC miner, “Avalon Miner” (Avalon A3256), was about 50-100 times more efficint than a typicalGPU and also the cost per GH/s was much lower than for a GPU.
        + Led to an increase from 20 TH/s (early 2013) to about 300 PH/s by end of 2014.

More than four orders of magnitude

* + - Continuous Growth (2014-2020)
      * Chip designs get better, but the mining manufacturers were also able to pay for better chip-processing manufacturers
        + More and smaller transistors on the same chip area.
        + Process Node

First generation ASIC chips were using a 110 (nanometer) process node, while modern ASICs use 7nm

About one hundred times more

* + - * (i) reducing the cost for hashrate and (ii) being more efficient.
        + Of 2020; 2 an improvement by a factor of 200.
        + Cost per TH/S to purchase the miners dropped by a factor of 500!
      * Between 2014 and the end of 2020, the network hashrate creased from 300 PH/s to about 135,000 PH s,
        + Price appreciation meant that bitcoin mining was extremely profitable
      * The end of 2020, here were approximately ten million machines distributed all over the world, keeping bitcoin safe.
  + 4.iii. Mining Costs
    - Two components for building and operating perspective there ares
      * Capital Expenditure (CapEx)
        + Buying the land and facilities to house the miners

Warehouses or containers

* + - * + Mining units themselves, substations and transformers, high voltage power cables, and cooling equipment. Of

Transforms power from high voltage (e.g., 115kV or more) to medium voltage (typically 2kV-3kV)

* + - * Operating Costs
        + Miners themselves use a tremendous amount of electricity, more consumed to keep them cool

Ongoing costs, such as taxes, the salaries of technicians and maintenance workers, management, administration and security costs. ` electricity.

Thus search for and use the cheapest available electricity sources.

* + - * Miner Efficiency
        + Constantly check whether it makes sense to upgrade
        + Might use the money she’d been spending on electricity to buy bitcoin rather than mine it.
      * Mining Dynamics
        + Incentivized to invest in more miners, raisthe network hashrate.
        + Hashrate will follow price movements. 109 The hashrate itself, however, does not have a direct effect on the bitcoin price.

Doesn’t drive the price, but the price can drive the nashrate.

* + - * + Block halving has a highly disruptive effect on the economics of mining, as revenue halves from one moment to the next.

Because the timing of this disruption is known and anticipated ell in advance, investment in mining equipment will take this nto account.

* + - * 4.iv. Geography:
        + Substantial part of the electricity used by miners is pent on cooling the machines, the colder the environment, the less expensive it is to mine for bitcoin. Consequently, many arge mining operations have chosen to set up or move north.
        + China, for example, having invested heavily in coal-burning power plants, has an over-supply of cheap elec ricity.

Manufacturers of ASIC miners is located there, made China an ttractive place for bitcoin mining operations, until it banned ptocurrency mining in mid-2021.

* + - * + Readily available hydroelectric power has also been a draw.

places like Washington State in the US, Quebec in Canada, several locations within Russia

* + - * + Generate income in bitcoin but must cover their costs in fiat currency (most often in US dollars).
* CHAPTER SUMMARY
  + Work is deliberately (and provably-hence the term proof of work) time- and energy-intensive, the first miner to solve each new block is rewarded with new bitcoins,
  + System rewards honest iners when they perform their role in reaching consensus in decentralized network.
  + A miner’s revenue is a function of the price of bitcoin in fiat currency and the network hashrate.
  + Unifies without centralizing.
  + Ultimate arbiter of truth.
    - Identical and constantly updated duplicates of itself on every node, it is both a shared memory and a linear history..
    - Governed by a set of principles that protect it against fragmentation.
    - Resistant to tampering

### Conclusion… 273

* Hope to leave you confident in your understanding not only of the bitcoin wonderland, but also the scope of its evolution and the derpinnings of its construction.
  + Monumental shift from a centralized to a decentralized world,
  + Potential to impact not only money, but, for xample, supply chains; contracts in the financial, real estate, any other industry; the internet of things; and decentraldecision-making.
* Decentralized proof of ownership is one promising application that has been pursued in various forms, with
  + Land registries, ownerof characters in computer games, and digital and realof
* Decentralized financial services
  + Borrowing and lending
  + Vithout the need for a bank or other financial institution as an termediary.
* When bitcoin was invented, most money was already digital
* Bringing ogthr popl with common intrsts rom all ovr th ri.
  + Privacy as a path to social and political change, a conversation began about how many of the internet’s virtues-the lack of a central authority and the possibility of anonymity prominent among them-might be brought to money.
* Like gold, bitcoin is scarce. Moreover, it is also carefully designed to be divisible, durable, portable, and fungible
  + Principles to be a better form of money, and to carry out the function of money more efficiently.
  + Sophisticated and technical, but not beyond an interested layperson’s grasp.
    - Is worth understanding, as is a critical part of our daily lives and historically many irrencies (e.g., the denarius) were debased and/or collapsed.
* Appreciate the origins, agenda, structure, and operation bitcoin. Offers not just a tate-free currency but a new way of conceptualizing money is as radical as it is elegant.
* Begins with an overview of oney’s history, learning its traits and function, and getting rasp of payment systems. H
* Radically creative impulse beautifully personified the mysterious figure of Satoshi Nakamoto.
  + Innovation fundamentally changes the way we think
  + Engineered to meet human economic needs and to out-perform by many metrics all currencies and payment systems that had come before it.
  + For all its engineering, bitcoin is remarkably easy to use.
    - Long as they take adequate care to protect their private key s, people can buy bitcoin from an ATM as easily as they can order Uber.
* Much the same way a person can drive without knowing much about how a car works, people can participate in bitcoin without knowing anything about cryptographic hash functions or blockchains.
  + 11 enhance your experience of using it.. I
* Inderstanding operates can increase your insight into the rapidly evolving future of many different aspects of the world above the rabbit ole and beyond the matrix.
* Envision a world where everyone can participate in (and enefit from) a decentralized monetary system.
  + This book as an effort to educate you about bitcoin and its dvantages-knowledge being an indispensable precondition the confident adoption of new technology.
  + If you found this &lt;valuable and it helped you to understand bitcoin, we have &gt;gether gotten closer to making that world a reality. 0