Appendix A

Appendix

A.1 Bitcoin: A Peer-to-Peer Electronic Cash System

Bitcoin is a decentralized digital currency that operates on a peer-to-peer network called the blockchain. It was introduced in a 2008 whitepaper by an anonymous person or group of people using the pseudonym Satoshi Nakamoto [5]. Bitcoin is not controlled by any central authority, such as a government or financial institution, making it a unique form of currency. It relies on cryptographic techniques to secure transactions and control the creation of new units.

What are the underlying technologies utilized by Bitcoin and what specific events occur during the transfer of a single Bitcoin from one digital wallet to another? In the upcoming sections, we aim to answer those questions.

A.1.1 How Does Bitcoin Actually Work?

Bitcoin's creation was prompted by the need for a secure and decentralized system of transferring value. The solution to this problem involved an intriguing mathematical puzzle that required the invention of new concepts such as digital signatures and cryptographic hash functions.

Creating a new cryptocurrency is a complex process that involves several steps, including developing a consensus mechanism, creating a blockchain, implementing security measures, and ensuring decentralization. To understand how Bitcoin works and identify potential areas for design improvements, it can be helpful to examine the technical details of its underlying protocols [5]. Alternative cryptocurrencies have emerged as a result of different design choices made by their creators, which has led to a diverse ecosystem of digital currencies with varying features and use cases.

While the underlying technology may seem complex to some, it is important to note that using a cryptocurrency does not require an in-depth understanding of its mechanics [96]. Just like swiping a credit card, users can take advantage of user-friendly applications that enable seamless sending and receiving of these digital assets.

The concept of cryptocurrency revolves around enabling individuals to conduct transactions without relying on a centralized entity for trust verification. Typically, when using a credit card to purchase goods or services, one must rely on banks (or a network of banks) to correctly debit the user's account and credit the recipient's account. The majority of currencies are issued by governments, which can exercise some level of control over their respective currencies through means such as adjusting the money supply. As a result, holders of these currencies must place a certain degree of trust in the government issuing them to manage them effectively.

The concept of Bitcoin was inspired by the desire to overcome the limitations of traditional financial systems. According to Nakamoto (2008, p.1) [5]:

> *the root problem with conventional currencies is all the trust that's required to make it work*

To address this issue, Bitcoin was designed as a decentralized digital currency that operates without a central authority or intermediary. The money supply of Bitcoin is fixed and determined by its underlying algorithm, making it resistant to inflation and manipulation. In addition, transactions in the Bitcoin network are recorded on a public ledger called the blockchain, which ensures transparency and accountability. Bitcoin allows for direct peer-to-peer payments without the need for intermediaries, such as banks or payment processors. This property of Bitcoin eliminates the need for trust in a central authority and enables participants to transact with each other directly, thereby reducing transaction costs and increasing efficiency.

The concept of decentralization in trustless payment systems has been subject to debate among readers. However, this discussion is beyond the scope of our current topic. While personal needs for trustless payments may vary, the question of whether such a system is technically feasible remains an intriguing one. Cryptography, which originated from encrypting messages, employs deep mathematical concepts to achieve its objectives. The remarkable effectiveness of cryptographic tools extends beyond confidential communication into other domains. For instance, the development of a decentralized currency presents a significant challenge that can be addressed by applying cryptographic techniques [97].

Creating Your Own Cryptocurrency

One common scenario where distributed ledgers can be useful is when multiple individuals frequently exchange small amounts of money, such as paying for shared expenses like dinner bills. To simplify this process, they may choose to maintain a communal ledger that records these transactions in a manner similar to using physical currency. By doing so, participants can easily keep track of their contributions and settle up when necessary.

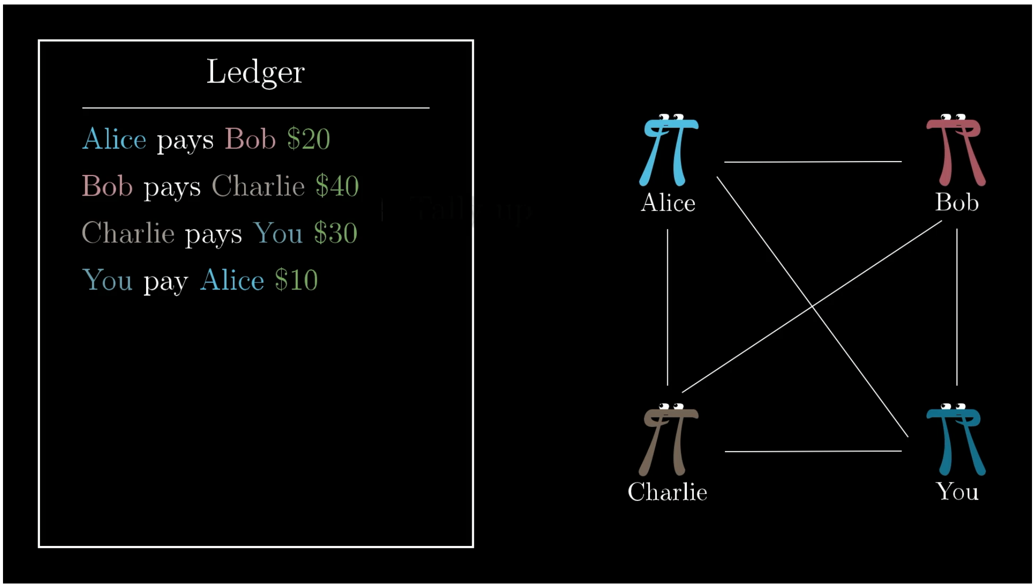


Figure A.1: A ledger is a record of financial transactions, utilized for monitoring the accounts of all parties involved (Reference: [98]).

The proposed ledger system would be a publicly accessible platform similar to a website where users can add new entries. At the end of each month, participants could review the list of transactions and calculate the total sum. If an individual has spent more than they have received, they would contribute that amount to the collective pool, while those who have received more than they have spent would withdraw funds from the pool.

The protocol for participation in the system involves the following steps:

1. Any individual can add entries to the distributed ledger;
2. At the end of each month, all participants gather to reconcile their accounts using physical currency.

However, a potential issue arises with a public ledger that allows any individual to add entries. How can one ensure that Bob does not enter "Alice pays Bob 100" without Alice's approval? There is a Cryptography solution: *Digital signatures.*

A.1.2 Digital Signatures

Digital signatures provide a means to ensure the authenticity and integrity of electronic transactions. The use of digital signatures allow recipients to verify that the information sent by a sender is what they intended to send, thereby establishing trust in the transaction [99].

The concept described here is similar to a handwritten signature, whereby Alice can add a message or proof of approval to a transaction that cannot be easily replicated by others. This is achieved through the use of digital signatures, which are based on cryptographic algorithms and provide a secure method for verifying the authenticity of a message or transaction [100]. The infeasibility of forging a signature is ensured through the use of advanced encryption techniques that make it difficult for unauthorized parties to tamper with or counterfeit digital signatures [100].

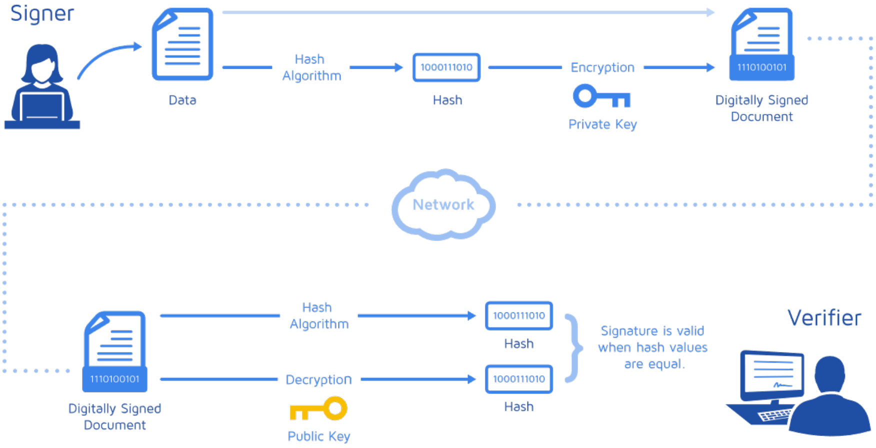


Figure A.2: Digital signature (Reference: [101]).

It may seem counterintuitive at first, but digital signatures can be implemented in a way that prevents forgery. In this context, a digital signature is a function of two elements: the private key, which only the signatory possesses, and the message being signed [97]. This means that even if an attacker were able to copy the initial signature, subsequent attempts to use it would result in a different value due to the unique relationship between the private key and the message.

In cryptography, a signature function is only effective if there exists a verification function to confirm its validity [102]. The mechanism for this involves generating a public-private key pair consisting of two strings of 1's and 0's. The private key, also known as the *secretkey*, is often abbreviated as *sk* while the public key is denoted as *pk*. As suggested by their names, the secret key should be kept confidential [103].

A digital signature scheme can be defined as a set of two operations: one for generating a digital signature on a given message, denoted as Sign, and the other for verifying the authenticity of a purported signature, denoted as Verify. These functions are typically implemented as follows:

1. *Signing function* Sign: This operation takes as input a message $m \in \{0,1\}^*$, and produces a digital signature Sign $\in \mathbb{Z}_q^*$, where q is a prime number. The security of the scheme is typically guaranteed by the assumption that it is computationally infeasible to compute the discrete logarithm in the underlying finite field, $\mathbb{Z}_q$.
2. *Verification function* Verify: This operation takes as input a message $m \in \{0,1\}^*$, a digital signature Sign $\in \mathbb{Z}_q^*$, and the public key (pk, sk), where $pk = g^x$ for some generator polynomial $g \in \mathbb{Z}[X]$ of degree $n-1$ and $x \in \mathbb{Z}_q$. The verification function outputs a Boolean value indicating whether or not the given signature is valid, i.e., $\text{Sign}(m) = g^y \mod q$, where $y \in \mathbb{Z}$ is the unique integer such that $g^{y \bmod n} \equiv sk \pmod{q}$.

The signing process requires employing the private key. The objective is that if Alice alone possesses her private key, then she is the only individual capable of generating a digital signature. If this key is compromised the security of the system is significantly undermined. The Verify function serves as a means of determining whether a given message bears a valid digital signature generated using the corresponding public key. It should return True when applied to an authentic signature and False for all other signatures.

The security of a digital signature scheme relies on the secrecy of the private key used to generate the signature. However, it is theoretically possible for an attacker to brute-force the public key and find a valid signature by exhaustively trying different potential signatures until one returns true [104]. In the case of Bitcoin's digital signature scheme, there are 2^{256} possible signatures due to the large number of bits in the hash function used for signature generation [103]. However, this number is so large that it makes brute-force attacks on the public key infeasible, providing a high level of security for Bitcoin's digital signatures.

A.1.3 Ledger

In blockchain systems, transactions are recorded on a distributed ledger and secured through cryptographic techniques. Specifically, each transaction needs to be signed by its corresponding private key, which ensures its authenticity and non-repudiation [99]. The signature generated for a given transaction is unique and dependent on the content of that transaction, making it impossible to reuse signatures from one transaction to another [105]. However, there is an issue with this approach. Suppose Alice signs a transaction, such as "Alice pays Bob $100", which is then recorded on the blockchain. Although Bob cannot forge Alice's signature on new messages, he could still copy that same line multiple times and submit it to the network. Since the message/signature combination is still valid, these duplicate transactions may be accepted by the network and included in its consensus state [106].

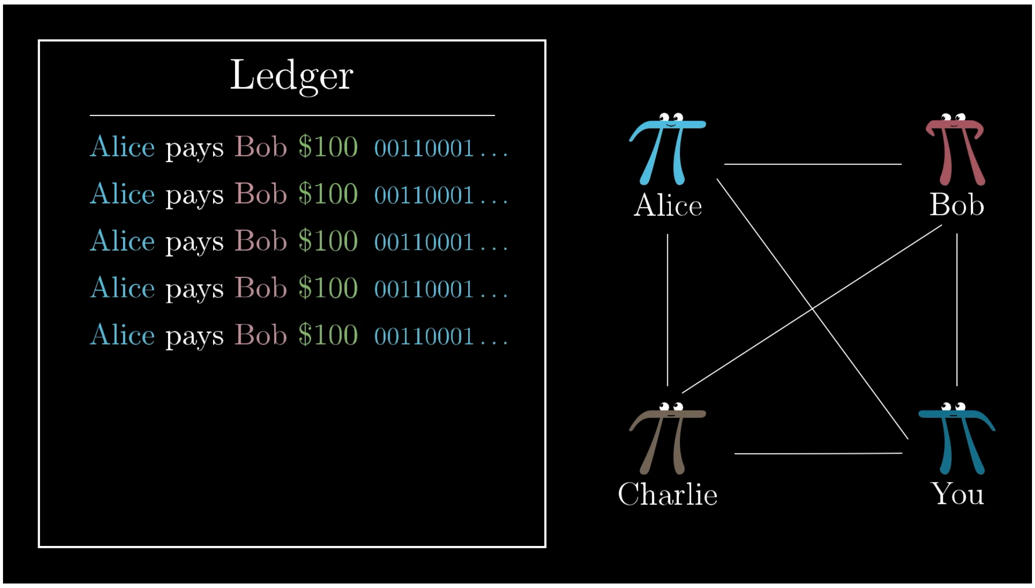

Ledger
Alice pays Bob $100 00110001...
Alice pays Bob $100 00110001...
Alice pays Bob $100 00110001...
Alice pays Bob $100 00110001...
Alice pays Bob $100 00110001...
Alice
Bob
Charlie
You

Figure A.3: Anyone can create copies of previous transactions (Reference: [107]).

The development of digital signatures can address the issue of trust in the initial protocol by introducing unique identifiers for transactions and requiring a distinct signature for each transaction. This approach has been proposed and implemented in various cryptographic systems, such as the RSA signature scheme [108] and the elliptic curve digital signature algorithm (ECDSA). The use of digital signatures not only enhances security but also enables efficient verification of the authenticity and integrity of electronic messages.

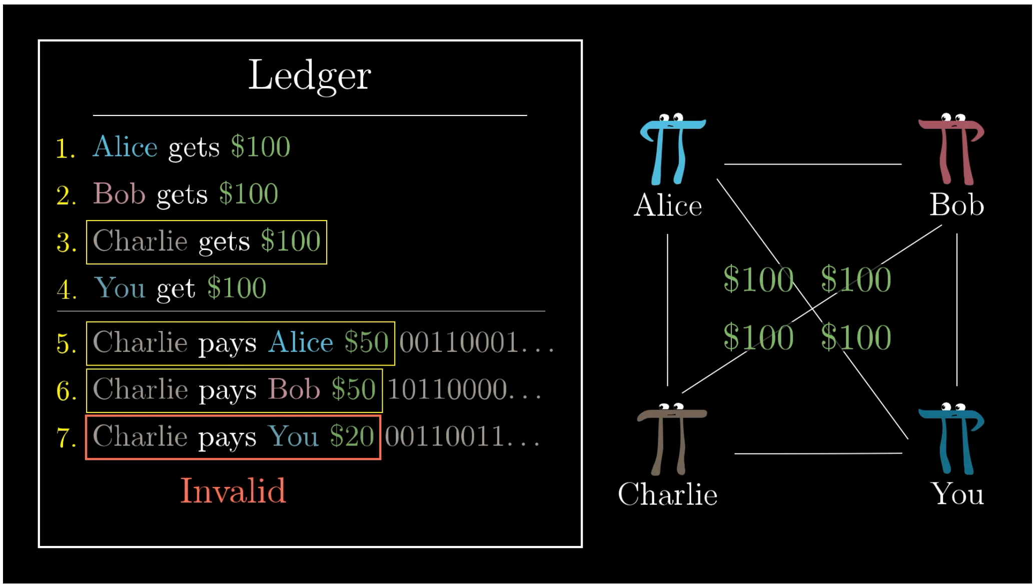
Removing Cash

The effectiveness of this system relies on an implicit agreement between individuals to uphold their financial obligations. Specifically, participants are expected to pay in cash at the end of each month, despite the absence of a formal enforcement mechanism. However, there is no guarantee that all parties will comply with this arrangement, as demonstrated by instances where one individual (e.g., Charlie) may accumulate significant debt and subsequently fail to fulfill their financial obligations.

In this cashless economic system, it may be necessary to revert to cash to settle up if certain individuals owe a significant amount of money (e.g., Charlie). However, as long as no one falls into debt and the ledger is properly maintained, the use of cash can be avoided. The ledger alone can function effectively as long as there is a mechanism in place to prevent excessive spending.

One strategy for managing a cashless economy without resorting to cash settlements is to have all participants deposit an equal amount (e.g., $100) into the pot, and record the initial distribution of funds on the ledger. For example, Alice would receive $100 in the first transaction, while Bob would receive $100 in the second transaction, and so on. By using this approach, individuals can maintain their financial balance without the need for cash transactions.

Now that we are under a cashless economic system, it is important to prevent double-spending attacks where a user attempts to spend the same cryptocurrency more than once. One way to accomplish this is by verifying that transactions are valid before they are added to the ledger. Specifically, if all users on the network start with zero balance ($0) and the first two transactions are of $100 value (Charlie pays Alice $50 and Charlie pays Bob $50), then a third transaction where Charlie pays You $20 would be invalid. This is because it violates the rule that a user cannot spend more than they have in their account.



Ledger

1. Alice gets $100
2. Bob gets $100
3. Charlie gets $100
4. You get $100

5. Charlie pays Alice $50 00110001...
6. Charlie pays Bob $50 10110000...
7. Charlie pays You $20 00110011...

Invalid

Figure A.4: In this new system, we don't allow people to spend more than they have. (Reference: [109]).

It can be noted that the requirement to ascertain the legitimacy of a transaction necessitates knowledge of the entire transaction history. This principle applies not only to traditional financial systems but also to decentralized digital currencies, although opportunities for improvement is present.

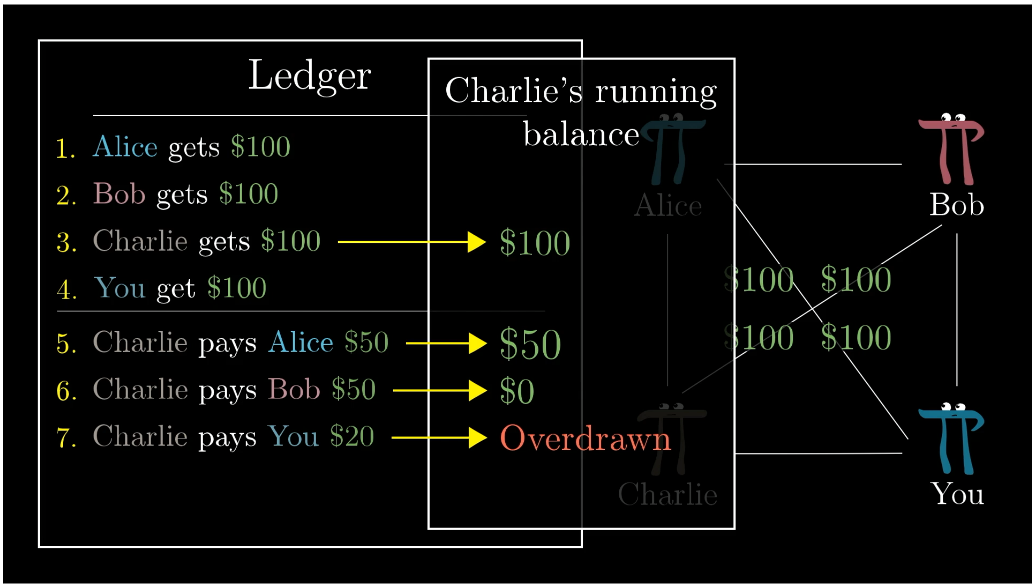


Figure A.5: Now verifying a transaction requires checking the entire ledger history to make sure nobody overdraws. (Reference: [110]).

The use of the above ledger system appears to dissociate it from physical cash transactions. If everyone in the world were to utilize this ledger, one could theoretically conduct all financial transactions solely through the ledger without any need for conversion to United States Dollars (USD). Many individuals currently perform digital transactions exclusively while occasionally using physical cash. The latter scenario involves a more intricate system of banks wherein the balance on a digital account can be converted into USD. However, if one and their associates were to completely detach their ledger from USD, there would be no guarantee that having a positive balance in the ledger could translate into physical currency in hand. To accentuate this point, one can stop using the $ sign, and digital quantities, on the ledger can be referred to as "Ledger Dollars" (LD).

Individuals possessing Ledger Dollars have the liberty to convert them into US dollars at their discretion. An example involves Alice offers Bob a zero-value US dollar bill in exchange for him adding and signing a transaction entry to the shared ledger, wherein Bob pays Alice ten units of Ledger Dollar value. However, the protocol does not explicitly guarantee the occurrence of such exchanges. Instead, it operates more similarly to foreign currency exchange in an open market where 10LD is its own independent entity. Additionally, if there is high demand for inclusion within the ledger, a transaction of 10LD may require a non-zero amount of physical cash. Conversely, if there is a low demand for participation, it may require only a minimal amount of physical cash.

Our ledger has been transformed into a form of currency that operates within a closed system, allowing for peer-to-peer transactions between individuals without the backing of a state or taxation imposed in the form of Ledger Dollars. It is important to recognize that, at its core, cryptocurrency can be viewed as a ledger that records the history of financial transactions, serving as the currency itself. The concept of possessing Bitcoin is simply represented by a positive balance on the Bitcoin ledger, which is associated with a secret key. This differs from traditional currency systems where money enters the ledger through cash transactions. In the case of Bitcoin, the process for introducing new money into the ledger will be discussed in more detail shortly. However, it is important to note that there are fundamental differences between Ledger Dollars and true cryptocurrencies.

Distributing The Ledger

The distributed nature of the blockchain technology used by the ledger system necessitates the use of a centralized platform for public access and modification of the ledger's contents. However, this raises concerns regarding the trustworthiness of the entity responsible for hosting the website and regulating the rules governing the addition of new entries to the ledger. In particular, it is important to identify and evaluate the credibility of the entity that controls the website and establishes the protocols for updating the ledger.

To eliminate trust in a centralized system where one ledger is maintained, we will replace this with a decentralized approach, where each individual will maintain their own copy of the ledger. This will enable transactions, such as "Alice pays Bob 100 LD" to be broadcasted and recorded on personal ledgers by all parties involved in the network.

The distributed ledger technology employed by Bitcoin involves the broadcast of transactions by users, which are then recorded on a decentralized set of records. This eliminates the need for trust in a central authority. However, this system is problematic due to the possibility of disagreement among participants regarding the correct ledger. For example, when Bob receives a transaction "Alice pays Bob 10 LD", how can he be certain that everyone else has received and believes in the same transaction? If even one person does not know about this transaction, they may not allow Bob to spend those 10 Ledger Dollars later.

The verification of the integrity and consensus of a blockchain network relies on a distributed ledger system where all participants maintain a copy of the same transaction history. The trustworthiness of this system is predicated on the assumption that all nodes will accurately record and remember past transactions, which may be subject to potential inconsistencies or discrepancies in the event of faulty or malicious behavior. Therefore, it

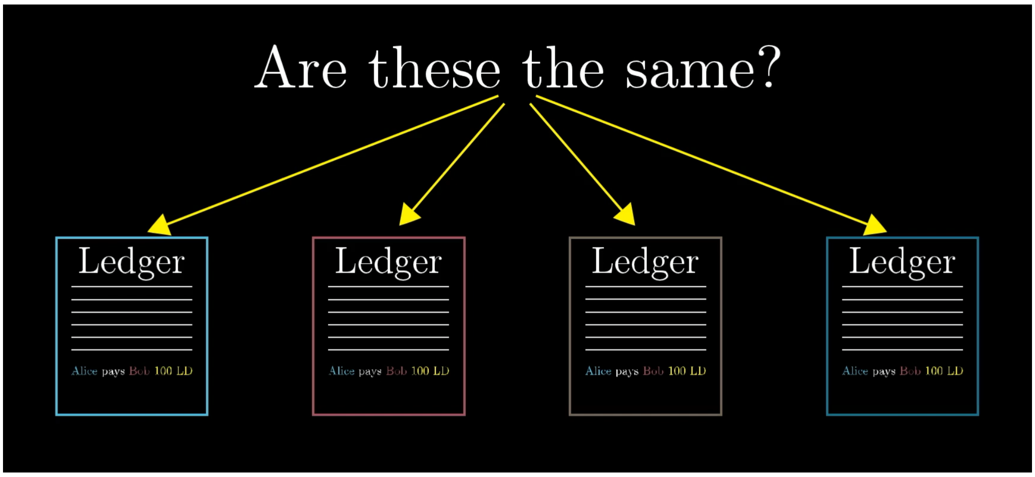


Figure A.6: If everyone keeps a unique copy of the ledger, how can we ensure that everybody agrees on what it should say? (Reference: [111]).

is essential to establish a mechanism for ensuring that the distributed ledger remains consistent across all participating nodes. The solution proposed by Satoshi Nakamoto in 2008 for decentralized systems was a method to validate the validity of a growing document, such as a ledger, without relying on a central authority. This problem was solved through the use of computational work to determine trustworthiness, where the ledger with the most computational effort invested in it is considered legitimate. The idea is that if an individual attempts to manipulate the ledger, it would require an impractical amount of computational power, making fraudulent transactions computationally infeasible. This concept forms the core of Bitcoin and other cryptocurrencies.

A.1.4 Hash Functions

Cryptographic hash functions are the primary tool utilized by Nakamoto's solution to this puzzle. These functions take in arbitrary messages or files as input and produce a fixed-length string of bits referred to as the "hash" or "digest" of the message, which is intended to exhibit randomness. The output of this process is deterministic and consistent for a given input, but minor alterations to the input can lead to drastically different hash values.

The property of unpredictability in the output changes when slightly changing the input is what makes SHA256 a cryptographic hash function [112]. This means that it is computationally infeasible to compute the original message from its hash value in reverse direction [113]. Therefore, given a specific hash value such as 1001111100111100 . . ., there is no efficient method to determine the corresponding input message other than brute-force guessing and checking with random inputs.

Given the provided function, what is the empirical evidence indicating a significant correlation between a specified set of Bitcoin transactions and an exceptional computational expenditure? *Proof-Of-Work*.

A.1.5 Proof-Of-Work

The task described involves manipulating a collection of transactions (enclosed within a container), whose hash value is computed utilizing the SHA256 algorithm. The objective is to modify a specified element within the container, such that the resulting hash commences with at least six consecutive zeros.

Achieving a solution to this problem is indeed possible, albeit requiring a considerable amount of time. Due to the inherent unpredictability of the hash function's output, the prevailing method for tackling this challenge remains a process of trial and error [114].

As the number of required leading zeroes increases, the difficulty of the problem escalates exponentially. Consider a scenario where an individual presents you with a list of transactions and asserts that they have identified a special number. They claim that by appending this number to the end of the transaction list and applying the SHA256 hash function to the entire sequence, the resulting output will exhibit 30 leading zero bits.

Assessing the level of difficulty involved in discovering the aforementioned number necessitates a thoughtful analysis. It is evident that the task likely posed significant challenges. When considering a randomly selected message, the probability of the resulting hash beginning with 30 consecutive zeroes is 1 in 2^{30}, which corresponds to approximately 1 in a billion [114]. Consequently, it is highly probable that the individual in question had to iterate through approximately one billion distinct guesses before successfully identifying this specific value.

Nevertheless, what proves intriguing is that once the number is known, its verification as a hash commencing with 30 zeros can be efficiently conducted. This verification process offers the ability to ascertain the substantial effort expended by the individual without necessitating the replication of the original labor. Termed as *proof-of-work*, this number holds significance.

It is crucial to emphasize that the entirety of this endeavor is intrinsically linked to the underlying list of transactions. Even a slight modification to any transaction would result in a completely altered hash, compelling a full repetition of the laborious process to identify a new number that yields a hash with 30 zeros [5].

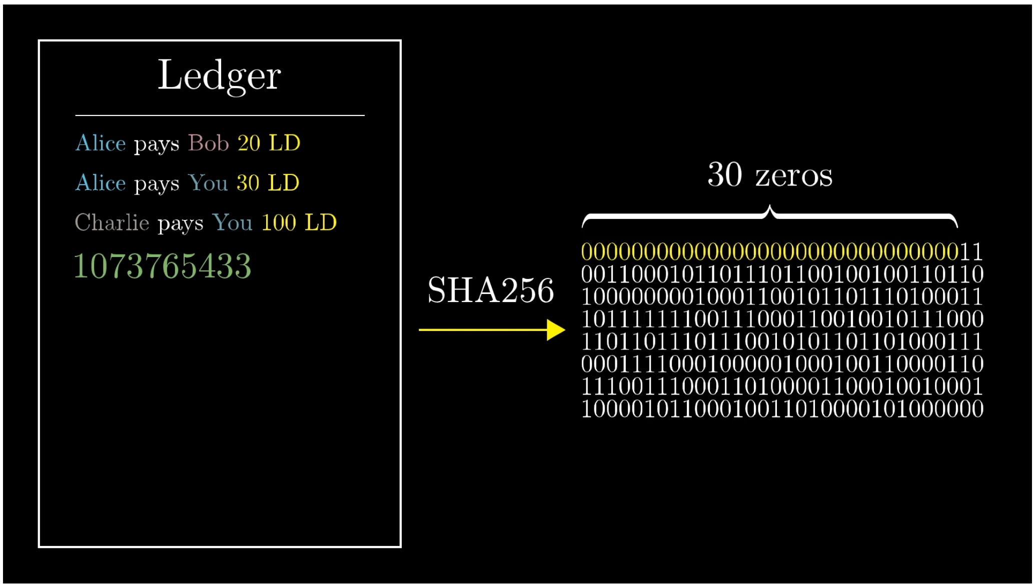


Figure A.7: There is no better way than guess and check for the special hash (Reference: [115]).

A.1.6 Blockchain

A distributed ledger system is composed of multiple nodes that broadcast transactions. To ensure consensus on the correct ledger, it is necessary to develop a mechanism that allows all nodes to agree on the validity of each transaction [116].

The core concept of the original Bitcoin paper [5] is based on the assumption that a distributed ledger will be trusted if it has been subject to a large amount of computational effort. This idea is implemented through the use of the many-zeroes game, which involves proving that a particular block in the chain contains a hash that is difficult to reverse-engineer.

Rather than hashing the entire ledger repeatedly, it is more efficient to allow for the accumulation of computational effort over time. Transactions are grouped into blocks and added to the chain in a linear fashion, with each new block containing a reference to the previous one. This approach allows for the creation of a tamper-evident history of transactions that is trusted by network participants due to the large amount of computational work required to manipulate it.

The block is a collection of transactions enclosed with a unique identifier, known as proof-of-work (PoW), which serves as evidence of the computational effort expended in validating the block. In PoW schemes, the miner must solve a complex mathematical problem to validate the block and add it to the blockchain. The difficulty level of this problem is determined by the target number of leading zeros required in the hash value of the block.

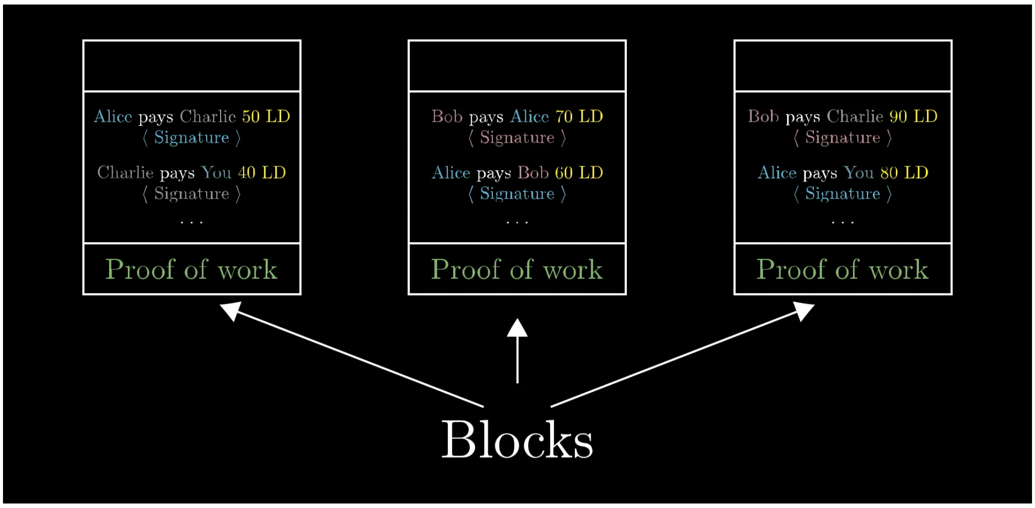


Figure A.8: Blocks on a blockchain (Reference: [117]).

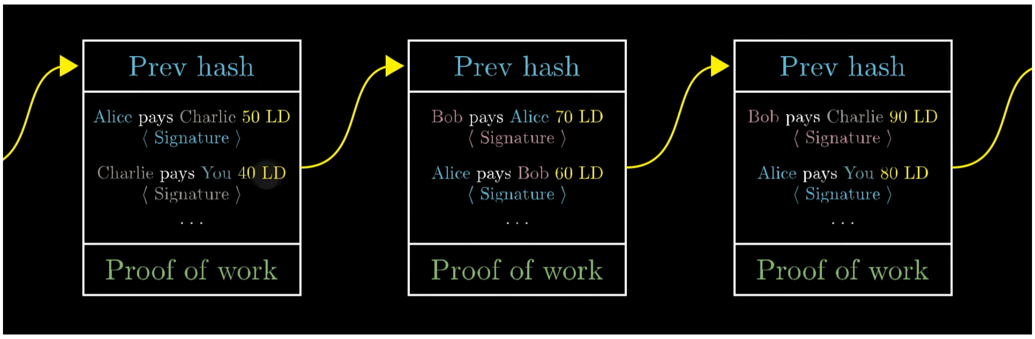


Figure A.9: Because blocks are chained together like this, instead of calling it a ledger, this is commonly called a “blockchain” (Reference: [118]).

A block is considered valid if it contains a proof-of-work (PoW) value, analogous to how a transaction is only considered valid when signed by its sender. Additionally, maintaining the integrity of the blockchain requires that blocks are not rearranged as this would disrupt the transaction history. To address this issue, each new block must begin with the hash of the previous block (hash-based chain), ensuring that the order of the blocks remains consistent.

Block Creators: Miners

To maintain the integrity of our ledger after it has been split into blocks, we have introduced a new process for adding new transactions. This involves grouping together transactions into blocks and computing a proof of work. As part of our updated protocol, anyone in the world is allowed to act as a "block creator". The responsibility of the block creator is to listen for broadcasted transactions, collect them into a block, and then perform a significant amount of computational work to find a special number that will result in the hash of the block starting with 60 zeros. This computed hash value is then broadcasted to the network as proof of work [119].

A special transaction can be included at the beginning of each block, where the creator is rewarded with a predetermined amount of digital currency. This practice has been suggested as a means of compensating individuals for their efforts in constructing blocks within a distributed ledger system [120].

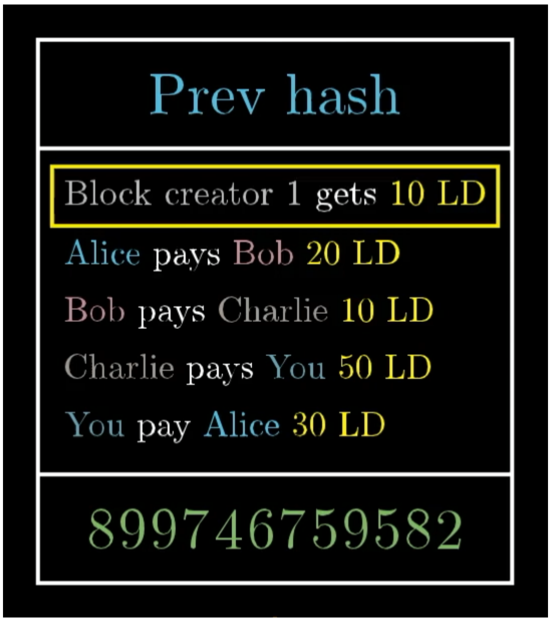


Figure A.10: Block reward (Reference: [121]).

The block reward is a unique exception to our usual transaction acceptance rules in the Ledger Dollar economy, as it does not require signature verification and increases the total number of currency units with each new block.

The process of creating blocks, known as "mining", involves a significant amount of work and introduces new currency into the economy. However, when discussing miners, it is essential to understand that they are primarily focused on listening to transactions, constructing blocks, broadcasting them, and receiving newly minted currency as a reward for their efforts.

For miners, each block can be thought of as a miniature lottery where individuals guess numbers rapidly until one person finds a combination that results in a hash starting with many zeros, earning the resulting reward. In contrast to mining, non-mining Bitcoin users no longer need to record all individual transactions on their personal ledger. Instead, they can simply monitor block production and rely on the fact that these blocks contain verified transactions. This approach is more manageable than maintaining a comprehensive transaction ledger.

In the consensus algorithm used by Bitcoin and other cryptocurrencies, a mechanism known as the "longest chain rule" is employed to resolve potential conflicts between competing blocks. Specifically, if two miners broadcast distinct blockchains with conflicting transaction histories, the system defers to the one that has been the longest in terms of cumulative proof-of-work effort expended on it, which is assumed to be more resistant to manipulation [122]. If there is a tie between two competing blocks, it may be necessary to wait for additional information to determine which block is longer. This process relies on the assumption that the longest chain represents the most widely accepted version of the blockchain. However, this approach has been subject to criticism due to its reliance on proof-of-work mechanisms, which require significant computational effort and can lead to centralization.

Attempt Fraud On The Blockchain

To evaluate the trustworthiness of this method, it is instructive to consider what steps an individual, such as Alice, would need to take in order to deceive the system. In particular, suppose that Alice desires to purchase an item from Bob for 100 Ledger Dollars (LD), but does not actually possess those LDs. She might attempt to send a block to Bob containing a line indicating "Alice pays Bob 100 LD" without broadcasting this block to the broader network. By doing so, Bob would believe that he had been paid and provide Alice with the item she desires. However, at a later time, Alice could re-enter the economy and spend those same 100 LD elsewhere. When Bob attempts to spending those same 100 LD, other individuals in the network may not recognize them as valid, leading to the potential for deception to be detected.

The process of creating a fraudulent transaction in a blockchain network requires a valid proof-of-work (PoW) that is found before other miners who are listening to the same set of transactions as the attacker, each working on their own block. This is a difficult task but can be accomplished if the attacker has a significant portion of the network's computation power. If Alice is able to find the PoW before other miners, she can create a fraudulent transaction and present it to Bob (but not to anyone else) [123].

However, Bob will continue to receive broadcasts from other miners, and Alice did not inform these miners about the block she produced for Bob. Therefore, they will not include this block in their own versions of the blockchain. As a result, Bob will be hearing conflicting chains: one from Alice and another from everyone else [124]. According to the protocol, Bob always trusts the longest chain he knows about, which may create challenges for detecting and resolving fraudulent transactions in the network.

The probability of Alice's computational resources being smaller than the combined computational resources of the rest of the network is high, and as a result, it is more likely for the rest of the network to find a valid proof of work for their next block before she does. Additionally, if Alice has less than 50% of the total computation on the network (which is highly probable), she will outpace everyone else indefinitely will be nearly impossible [5].

Eventually, when Alice fails to maintain her chain longer than the rest of the network, Bob will reject what he is hearing from Alice and follow the longer chain that everyone else is working on. This is because creating blocks requires significant computational effort, making it extremely difficult for any individual or group to manipulate the consensus [125].

It's worth noting that while building a single fraudulent block may be possible, maintaining the lie for an extended period is challenging. Therefore, users should exercise caution and wait for several new blocks to be added on top of a newly discovered block before trusting it as part of the main chain. By doing so, they can ensure that they are not being tricked by a malicious actor attempting to manipulate the network [126].

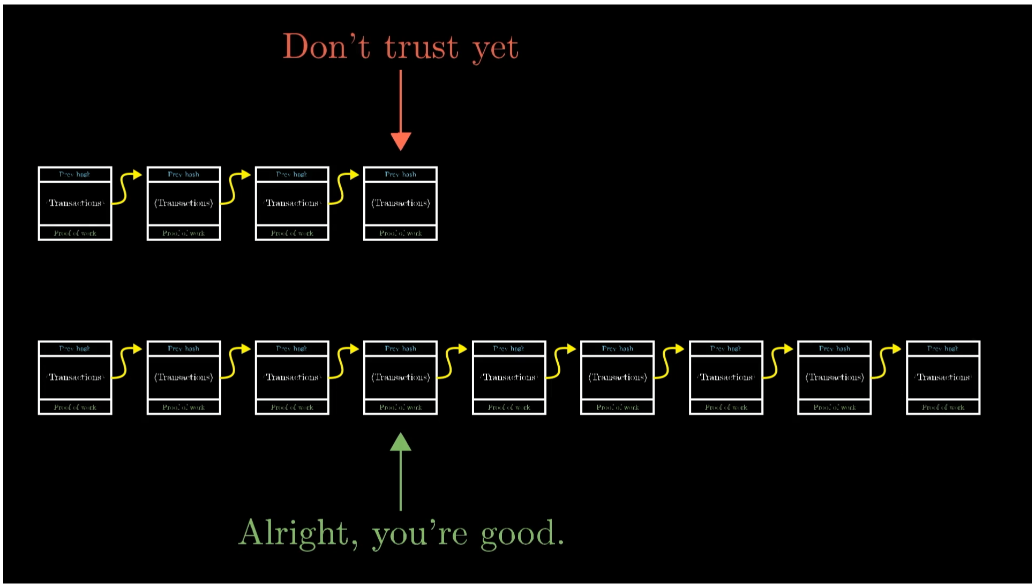


Figure A.11: Blocks are most trustworthy when they aren't brand new (Reference: [127]).

Ledger Dollars vs. Bitcoin

The distributed ledger system based on proof-of-work, as demonstrated by Bitcoin and other cryptocurrencies, involves a mining process where miners compete to solve a computational puzzle in order to validate transactions and add them to the blockchain. This is accomplished through the use of hash functions, which are designed to be difficult to reverse engineer, thereby ensuring the integrity of the distributed ledger [128]. The proof-of-work challenge may involve finding a special number that will make the hash of the block start with 60 zeros. However, in practice, this is achieved by systematically changing the number of zeros so that it takes approximately 10 minutes for miners to find a new block [5].

As a result of this process, a block reward is awarded to the miner who successfully validates a block. Initially, the reward was set at 50 Bitcoin per block, but it has since been reduced to 6.25 Bitcoin per block every 210,000 blocks [5]. However, miners can also earn transaction fees by including them in the validation process of transactions.

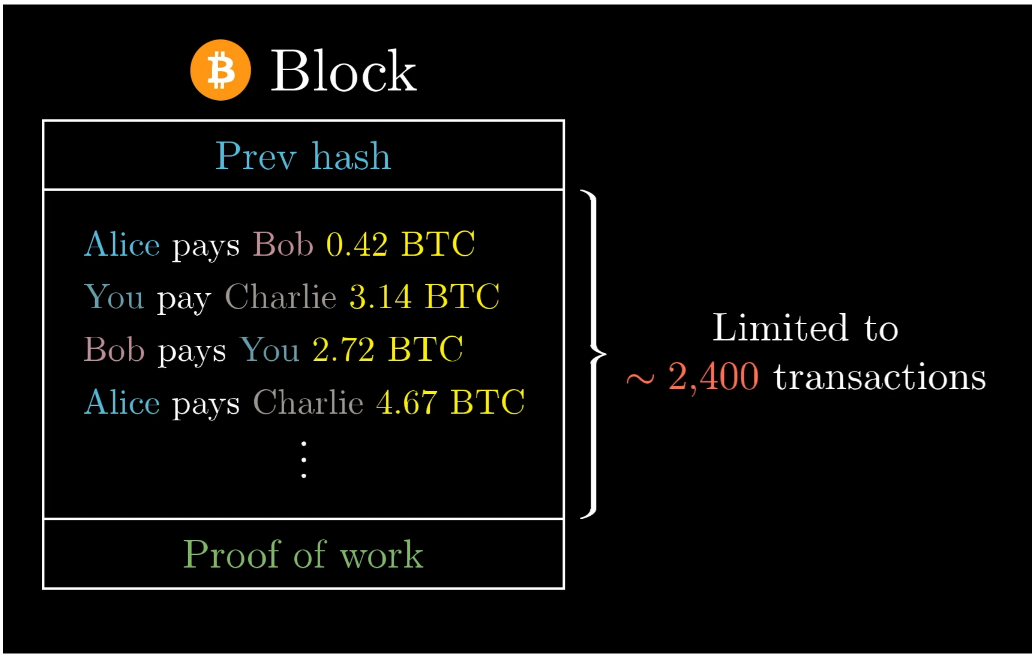


Figure A.12: Transactions on a bitcoin blockchain is limited (Reference: [129]).

Considering Bitcoin's objective of approximately one block addition per 10 minutes, its processing capacity is constrained to about 4 Bitcoin transactions per second, with some variability. By comparison, Visa handles an average of approximately 1,700 transactions per second, with the capability to process over 24,000 per second. The relatively slower processing speed of Bitcoin leads to higher transaction fees, as they determine the selection of transactions included in new blocks by miners. Moreover, Bitcoin has faced criticism for its significant energy consumption. While the proof-of-work concept effectively combats fraud, it necessitates an immense allocation of resources for block mining.

According to the Cambridge Bitcoin Electricity Consumption Index, the present annual electricity consumption for Bitcoin mining (as of 2021) is estimated at around 115 Terrawatt-Hours. To provide context, this consumption surpasses the energy usage of the entire country of Finland. Since 2008, an alternative approach to proof of work, known as "proof of stake," has emerged, offering a substantial reduction in energy requirements. Several newer cryptocurrencies have embraced this methodology [130].

References

[1] Diamond, Douglas W and Philip H Dybvig: *Bank runs, deposit insurance, and liquidity.* Journal of political economy, 91(3):401–419, 1983. 1

[2] Minsky, Hyman P and Henry Kaufman: *Stabilizing an unstable economy*, volume 1. McGraw-Hill New York, 2008. 2

[3] Bordo, Michael D: *An historical perspective on the crisis of 2007-2008.* Technical report, National Bureau of Economic Research, 2008. 2

[4] Murphy, Austin: *An analysis of the financial crisis of 2008: causes and solutions.* An Analysis of the Financial Crisis of, 2008. 2

[5] Nakamoto, Satoshi: *Bitcoin: A peer-to-peer electronic cash system.* 2008. `https://bitcoin.org/bitcoin.pdf`. 2, 5, 37, 38, 47, 48, 52, 53

[6] Zhang, Xiaojun, Ying Wen, Jie Zhou, Wei Zhang, and Xiaofeng Liao: *Financial fraud detection in cryptocurrency exchanges: A comprehensive survey.* IEEE Access, 8:193150–193172, 2020. 2

[7] Zainal, Anazida, Joarder Kamruzzaman, and Ruhul A Sarker: *A review on machine learning techniques for the detection of financial statement fraud.* International Journal of Financial Studies, 6(3):70, 2018. 2

[8] Hasbrouck, Joel and Gideon Saar: *Spoofing and layering in high-frequency trading.* Journal of Financial Markets, 16(4):646–679, 2013. 2

[9] Brogaard, Jonathan and Terrence Hendershott: *Market manipulation and high-frequency trading.* The Journal of Finance, 69(4):1637–1670, 2014. 3

[10] Bhattacharyya, Siddhartha, Sanjay Jha, and Kurian Tharakunnel: *A survey of data mining techniques for fraud detection.* ACM Computing Surveys (CSUR), 43(4):26, 2011. 3

[11] Smith, Adam: *The Wealth of Nations: An inquiry into the nature and causes of the Wealth of Nations.* Harriman House Limited, 2010. 5, 7

[12] Durlauf, Steven and Lawrence E Blume: *The new Palgrave dictionary of economics.* Springer, 2016. 6

[13] Goodhart, Charles AE: *The two concepts of money: implications for the analysis of optimal currency areas.* European journal of political economy, 14(3):407–432, 1998. 6

[14] Meneses, Italo Bezerra de: *On the origins of money.* MISES: Interdisciplinary Journal of Philosophy, Law and Economics, 4(2):585–587, 2016. 6

[15] Polanyi, Karl: *Trade and market in the early empires: Economies in history and theory.* 1965. 7

[16] Graeber, David: *Debt: The first 5000 years.* Penguin UK, 2012. 7

[17] Ricardo, David: *On the principles of political economy.* J. Murray London, 1821. 7

[18] Marshall, Alfred: *Principles of economics: unabridged eighth edition.* Cosimo, Inc., 2009. 7

[19] Klein, P.G.: *Principles of Economics.* Ludwig von Mises Institute, 2011, ISBN 9781610162029. `https://books.google.com.br/books?id=GYjEtAEACAAJ`. 7

[20] Hicks, John R: *Theory of employment, interest and money.* The Economic Journal, 46(182):238–253, 1936. 7

[21] Li, Xiuhua: *The formation and spread of the ancient chinese coinage system.* East Asian Archaeology, 3(1):95–106, 2003. 7

[22] Hartill, David: *Cast Chinese Coins.* Trafford Publishing, 2nd edition, 2005. 7

[23] Cribb, Joe: *Money: From Cowrie Shells to Credit Cards.* British Museum Press, 1991. 7

[24] Vries, Ad de: *The Industrial Revolution and the Industrious Revolution.* Cambridge University Press, 2008. 7

[25] Weatherford, Jack: *The History of Money.* Crown Business, 1997. 8

[26] Ferguson, Niall: *The Ascent of Money: A Financial History of the World.* Penguin Books, 2009. 8

[27] Graeber, David: *Debt: The First 5000 Years.* Melville House, 2011. 8, 9

[28] Ingham, Geoffrey: *The nature of money.* Polity, 36(3):387–412, 2004. 8

[29] Goodhart, Charles: *The Two Concepts of Money: Implications for the Analysis of Optimal Currency Areas.* European University Institute, 1998. 8

[30] Gupta, Chirag: *The myth of intrinsic value: The case of fiat money.* Journal of Interdisciplinary Economics, 31(2):177–195, 2019. 8

[31] Reinhart, Carmen M. and Kenneth S. Rogoff: *This Time Is Different: Eight Centuries of Financial Folly.* Princeton University Press, 2018. 8

[32] Friedman, Milton: *The role of government in education.* Economic Affairs, 20(4):4–8, 2000. 8

[33] Mankiw, N. Gregory: *Principles of Macroeconomics.* Cengage Learning, 2014. 9

[34] Blinder, Alan S.: *Quantitative easing: Entrance and exit strategies.* The Economic Journal, 120(519):50–51, 2010. 9

[35] Fund, International Monetary: *World economic outlook, october 2020: A long and difficult ascent.* 2020. 9

[36] Blinder, Alan S.: *The covid-19 crisis: Economic policy implications.* NBER Working Paper Series, w26935, 2020. 9

[37] Federal Reserve System, Board of Governors of the: *Money stock and debt measures h.6 release.* 2023. `https://www.federalreserve.gov/releases/h6/current/default.htm`. 9

[38] Blanchard, Olivier: *Inflation expectations and uncertainty in the time of covid-19: An overview.* NBER Working Paper Series, w28106, 2021. 9

[39] Labor Statistics, Bureau of: *Consumer price index summary.* 2023. `https://www.bls.gov/news.release/cpi.nr0.htm`. 9

[40] Office, Congressional Budget: *The macroeconomic effects of the american rescue plan act.* 2020. 9

[41] Kahn, Lisa B. and Bhashkar Mazumder: *Job loss and reservation wages during the covid-19 recession.* Brookings Papers on Economic Activity, 51(1):289–356, 2020. 9

[42] Labor, United States Department of: *Minimum wages for tipped employees.* 2023. `https://www.dol.gov/agencies/whd/state/tipped`. 9

[43] Labor Statistics, Bureau of: *Occupational employment and wages, may 2022.* 2022. `https://www.bls.gov/oes/2022/may/oes356011.htm`. 10

[44] Azar, Ariel and Ioana E. Marinescu: *Labor market concentration.* NBER Working Paper Series, w26634, 2020. 10

[45] Federal Reserve System, Board of Governors of the: *The federal reserve system: Purposes and functions.* 2021. `https://www.federalreserve.gov/aboutthefed/pf.htm`. 10

[46] Office, Congressional Budget: *Policies that would increase economic output and employment in the short term.* 2021. 10

[47] Treasury, U.S. Department of the: *The debt to the penny and who holds it.* 2023. `https://www.treasurydirect.gov/NP/debt/current`. 10

[48] Treasury, U.S. Department of the: *Treasury securities.* 2023. `https://home.treasury.gov/policy-issues/financial-markets-financial-institutions-and-fiscal-service/public-debt`. 10

[49] Federal Reserve System, Board of Governors of the: *Monetary policy and inflation.* 2022. `https://www.federalreserve.gov/monetarypolicy/inflation.htm`. 10

[50] Federal Reserve System, Board of Governors of the: *Statement on longer-run goals and monetary policy strategy.* 2020. https://www.federalreserve.gov/monetarypolicy/review-of-monetary-policy-strategy-tools-and-communications-statement-on-longer-htm. 10

[51] Lavoie, Michel: *Currency devaluation and domestic output.* Review of Political Economy, 6(3):309–319, 1994. 11

[52] Bernanke, Ben S.: *The global saving glut and the u.s. current account deficit.* Board of Governors of the Federal Reserve System, 2005. https://www.federalreserve.gov/boarddocs/speeches/2005/200503102/default.htm. 11

[53] Shiller, Robert J.: *Irrational exuberance.* The Economic Journal, 111(471):652–653, 2001. 11

[54] Mankiw, N. Gregory: *Principles of Macroeconomics.* Cengage Learning, 7th edition, 2014. 11

[55] Friedman, Milton: *Money: M1, m2, and m3.* The Journal of Political Economy, 112(2):S117–S134, 2004. 11

[56] Domanski, Dietrich and Vladyslav Sushko: *Currency manipulation: The imf and wto.* BIS Quarterly Review, September:79–91, 2011. 12

[57] Goldstein, Morris and Nicholas R. Lardy: *Currency manipulation: The imf and wto.* Peterson Institute for International Economics Policy Brief, 2018. https://www.piie.com/publications/policy-briefs/currency-manipulation-imf-and-wto. 12

[58] Karim, Mohamed A and Samah Mikhael: *Manipulation detection in cryptocurrency markets.* IEEE Access, 6:11044–11054, 2018. 12

[59] Cheah, Eng Tuck and John Fry: *Pump and dump schemes in cryptocurrency markets.* Social Science Research Network, 2015. 12

[60] Jin, Xinghua, Xiaohua Cheng, Qian Su, and Ting Liu: *Pump-and-dump manipulation in cryptocurrency markets.* Information Systems Frontiers, 22(6):1389–1402, 2020. 13

[61] Yang, Yuxing, Yi Zhang, and Yang Yang: *Pump and dump on the cryptocurrency market: Evidence from cryptocurrency telegram groups.* Journal of Corporate Finance, 56:228–248, 2019. 13

[62] Gandal, Neil, JT Hamrick, Tyler Moore, and Tali Oberman: *Price manipulation in the bitcoin ecosystem.* In *Proceedings of the 2018 Conference on Economic and Financial Computing*, pages 1–7, 2018. 13, 14, 22

[63] Edelman, Benjamin, Tyler Moore, and Tali Oberman: *Detecting pump and dump in cryptocurrency markets.* Journal of Economic Perspectives, 32(2):81–102, 2018. 13, 14

[64] Van Loon, Sander, Harald Vranken, and William Knottenbelt: *Front-running in permissionless decentralized exchanges.* IEEE Transactions on Dependable and Secure Computing, 18(1):305–318, 2021. 14

[65] Bistarelli, Stefano, Maurizio Naldi, Federica Paci, and Fiammetta Rossi: *Front-running and self-trading in permissionless blockchains.* In *2018 IEEE International Conference on Blockchain (Blockchain)*, pages 541–548, 2018. 14

[66] Chai, Daniel, Frank Fehle, and Cameron Truong: *Insider trading in the market for initial coin offerings: Evidence from pre- and post-launch trading.* Journal of Corporate Finance, 56:402–424, 2019. 15

[67] Liu, Yuxin, Xin Su, and Zhong Liu: *Detecting insider trading from blockchain ecosystem.* IEEE Access, 8:161071–161080, 2020. 15

[68] Yang, Sisi, Ling Zhu, Zhe Wu, and Yongfeng Huang: *Spreading bad news or rumors? analysis of cryptocurrency market manipulation on twitter.* IEEE Transactions on Knowledge and Data Engineering, 2021. 15

[69] Feng, Ling, Zheng Li, Kevin Yang, and Chao Zhang: *Cryptocurrency market manipulation: Evidence from twitter.* Pacific-Basin Finance Journal, 64:101384, 2020. 15

[70] Corwin, Shane A. and Paul Schultz: *The role of ipo underwriting syndicates: Pricing, information production, and underwriter competition.* Journal of Finance, 67(5):1767–1808, 2012. 16

[71] Jarrow, Robert A. and Philip Protter: *A dysfunctional role of high frequency trading in electronic markets.* Quantitative Finance, 11(8):1197–1214, 2011. 16

[72] *The cftc orders five banks to pay over $1.4 billion in penalties for attempted manipulation of foreign exchange benchmark rates.* 2018. `https://www.cftc.gov/PressRoom/PressReleases/7874-18`. 16

[73] *Sec charges 14 firms in $14.4 million layering scheme.* 2015. `https://www.sec.gov/news/pressrelease/2015-46.html`. 16

[74] *Two former deutsche bank traders convicted in connection with scheme to manipulate the u.s. dollar libor and euro interbank offered rate.* 2018. `https://www.justice.gov/opa/pr/two-former-deutsche-bank-traders-convicted-role-scheme-manipulate-critical-globa` 16

[75] *Cftc orders merrill lynch commodities, inc. to pay $25 million penalty for spoofing in precious metals futures contracts.* 2019. `https://www.cftc.gov/PressRoom/PressReleases/7972-19`. 16

[76] Trillium Management, LLC: *Surveyor-illustrations-template-1.jpg.* `https://www.trlm.com/wp-content/uploads/2016/08/Surveyor-Illustrations-Template-1.jpg`, visited on 2023-06-18. 17

[77] Corcoran, Conor and Paul Green: *Understanding hft spoofing and layering techniques.* Journal of Financial Market Infrastructures, 8(4), 2020. 17

[78] Cheung, Adrian, Wing S. Chow, and Jacky C. K. Cheung: *Understanding high-frequency trading in the cryptocurrency market.* IEEE Transactions on Computational Social Systems, 6(1):47–61, 2019. 17

[79] Trillium Management, LLC: *Surveyor-illustrations-template.jpg.* `https://www.trlm.com/wp-content/uploads/2016/08/Surveyor-Illustrations-Template.jpg`, visited on 2023-06-18. 17

[80] Commission, U.S. Commodity Futures Trading: *Cftc orders mizuho bank, ltd. to pay $250,000 for spoofing and attempted manipulation in the precious metals futures markets.* 2018. `https://www.cftc.gov/PressRoom/PressReleases/7831-18`, visited on 2021-09-17. 18

[81] Lu, David Z.: *Individual accountability for corporate wrongdoing.* Notre Dame Law Review, 96(5):1991–2044, 2021. 18

[82] Schultz, Thomas J.: *Spoofing and manipulation in commodity futures markets.* Fordham Journal of Corporate & Financial Law, 24:1–59, 2019. 18

[83] Andrews, Neil: *The cftc fights spoofing in the futures markets.* The Review of Securities & Commodities Regulation, 51(14):1–14, 2018. 18

[84] Doherty, Robert W. and Kathleen M. Mowry: *Taming spoofing: The pursuit of criminals in the futures markets.* The Review of Securities & Commodities Regulation, 52(17):1–12, 2019. 18

[85] Chilton, Bart: *Perspectives on high-frequency trading regulation.* Stanford Journal of Law, Business & Finance, 17(2):261–276, 2012. 19

[86] Angel, James J. and James A. McCabe: *Spoofing and layering.* University of Pennsylvania Law Review, 168(4):751–810, 2020. 19

[87] Cataldo, Anthony: *Making the case for a financial transaction tax.* Fordham Journal of Corporate & Financial Law, 25(1):97–144, 2019. 19

[88] Hevner, Alan, Samir Chatterjee, Alan Hevner, and Samir Chatterjee: *Design science research in information systems.* Design research in information systems: theory and practice, pages 9–22, 2010. 22

[89] Peffers, Ken, Tuure Tuunanen, Marcus A Rothenberger, and Samir Chatterjee: *A design science research methodology for information systems research.* Journal of management information systems, 24(3):45–77, 2007. 22

[90] Cartea, Álvaro, Sebastian Jaimungal, and Damir Kinzebulatov: *Algorithmic trading with learning.* International Journal of Theoretical and Applied Finance, 19(04):1650028, 2016. 22

[91] Chan, Stephen, Jeffrey Chu, Saralees Nadarajah, and Joerg Osterrieder: *A statistical analysis of cryptocurrencies.* Journal of Risk and Financial Management, 10(2):12, 2017. 22

[92] Vaswani, Ashish, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan N Gomez, Łukasz Kaiser, and Illia Polosukhin: *Attention is all you need.* Advances in neural information processing systems, 30, 2017. 23

[93] Howard, Jeremy and Sebastian Ruder: *Universal language model fine-tuning for text classification.* arXiv preprint arXiv:1801.06146, 2018. 23

[94] Barocas, Solon, Moritz Hardt, and Arvind Narayanan: *Fairness in machine learning.* Nips tutorial, 1:2017, 2017. 24

[95] Mittelstadt, Brent Daniel, Patrick Allo, Mariarosaria Taddeo, Sandra Wachter, and Luciano Floridi: *The ethics of algorithms: Mapping the debate.* Big Data & Society, 3(2):2053951716679679, 2016. 24

[96] Barski, Conrad and Chris Wilmer: *Bitcoin for the Befuddled.* No starch press, 2014. 38

[97] Diffie, Whitfield and Martin E Hellman: *New directions in cryptography.* In *Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman*, pages 365–390. 2022. 38, 40

[98] Sanderson, Grant: *ledger.png.* `https://3b1b-posts.us-east-1.linodeobjects.com//content/lessons/2017/bitcoin/ledger.png`, visited on 2023-06-01. 39

[99] Stinson, Douglas Robert and Maura Paterson: *Cryptography: theory and practice.* CRC press, 2018. 40, 41

[100] ElGamal, Taher: *A public key cryptosystem and a signature scheme based on discrete logarithms.* IEEE transactions on information theory, 31(4):469–472, 1985. 40

[101] DocuSign, Inc: *ds_subpage_diagram2.svg.* `https://www.docusign.com/static-c-assets/ds_subpage_diagram2.svg`, visited on 2022-06-04. 40

[102] Stallings, William: *Cryptography and network security principles and practices*, 2006. 40

[103] Barker, Elaine: *Digital signature standard (dss)*, 2013-07-19 2013. 40, 41

[104] Boneh, Dan, Ben Lynn, and Hovav Shacham: *Short signatures from the weil pairing.* In *Advances in Cryptology—ASIACRYPT 2001: 7th International Conference on the Theory and Application of Cryptology and Information Security Gold Coast, Australia, December 9–13, 2001 Proceedings 7*, pages 514–532. Springer, 2001. 41

[105] Bruce, Schneier: *Applied cryptography: Protocols, algorthms, and source code in c.-2nd*, 1996. 42

[106] Swan, Melanie: *Blockchain: Blueprint for a new economy.* 2015. `https://www.oreilly.com/library/view/blockchain-blueprint-for/9781491920459/`. 42

[107] Sanderson, Grant: *duplicate-transaction.png.* `https://3b1b-posts.us-east-1.linodeobjects.com//content/lessons/2017/bitcoin/duplicate-transaction.png`, visited on 2023-06-05. 42

[108] Rivest, Ronald L, Adi Shamir, and Leonard Adleman: *A method for obtaining digital signatures and public-key cryptosystems.* Communications of the ACM, 21(2):120–126, 1978. 42

[109] Sanderson, Grant: *invalid.png.* `https://3b1b-posts.us-east-1.linodeobjects.com//content/lessons/2017/bitcoin/invalid.png`, visited on 2023-06-05. 43

[110] Sanderson, Grant: *overdrawn.png.* `https://3b1b-posts.us-east-1.linodeobjects.com//content/lessons/2017/bitcoin/overdrawn.png`, visited on 2023-06-05. 44

[111] Sanderson, Grant: *ledgers.png.* `https://3b1b-posts.us-east-1.linodeobjects.com//content/lessons/2017/bitcoin/are-these-the-same.png`, visited on 2023-06-05. 46

[112] Dang, Quynh H: *Secure hash standard.* 2015. 46

[113] Butin, Denis: *Hash-based signatures: State of play.* IEEE security & privacy, 15(4):37–43, 2017. 46

[114] Dworkin, Morris: *Sha-256 hash function.* NIST FIPS, 180-4, 2001. `https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf`. 47

[115] Sanderson, Grant: *guess-and-check.png.* `https://3b1b-posts.us-east-1.linodeobjects.com//content/lessons/2017/bitcoin/30-zeroes.png`, visited on 2023-06-06. 48

[116] El Ioini, Nabil and Claus Pahl: *A review of distributed ledger technologies.* In *On the Move to Meaningful Internet Systems. OTM 2018 Conferences: Confederated International Conferences: CoopIS, C&TC, and ODBASE 2018, Valletta, Malta, October 22-26, 2018, Proceedings, Part II*, pages 277–288. Springer, 2018. 48

[117] Sanderson, Grant: *blocks.png.* `https://3b1b-posts.us-east-1.linodeobjects.com//content/lessons/2017/bitcoin/blocks.png`, visited on 2023-06-06. 49

[118] Sanderson, Grant: *block-ordering.png.* `https://3b1b-posts.us-east-1.linodeobjects.com//content/lessons/2017/bitcoin/block-ordering.png`, visited on 2023-06-06. 49

[119] Wood, Gavin *et al.*: *Ethereum: A secure decentralised generalised transaction ledger.* Ethereum project yellow paper, 151(2014):1–32, 2014. 50

[120] Ding, Xingjian, Jianxiong Guo, Deying Li, and Weili Wu: *An incentive mechanism for building a secure blockchain-based internet of things.* IEEE Transactions on Network Science and Engineering, 8(1):477–487, 2020. 50

[121] Sanderson, Grant: *block-reward.png.* `https://3b1b-posts.us-east-1.linodeobjects.com//content/lessons/2017/bitcoin/block-reward.png`, visited on 2023-06-06. 50

[122] Buterin, Vitalik *et al.*: *A next-generation smart contract and decentralized application platform.* white paper, 3(37):2–1, 2014. 51

[123] Fang, Fan, Carmine Ventre, Michail Basios, Leslie Kanthan, David Martinez-Rego, Fan Wu, and Lingbo Li: *Cryptocurrency trading: a comprehensive survey.* Financial Innovation, 8(1):1–59, 2022. 51

[124] Tan, Evrim, Stanislav Mahula, and Joep Crompvoets: *Blockchain governance in the public sector: A conceptual framework for public management.* Government Information Quarterly, 39(1):101625, 2022, ISSN 0740-624X. `https://www.sciencedirect.com/science/article/pii/S0740624X21000617`. 51

[125] Szabo, Nick: *Bit gold.* Recuperado de https://nakamotoinstitute. org/bit-gold/TVer página, 2005. 52

[126] DuPont, Quinn: *Cryptocurrencies and blockchains.* John Wiley & Sons, 2019. 52

[127] Sanderson, Grant: *dont-trust-yet.png.* `https://3b1b-posts.us-east-1.linodeobjects.com//content/lessons/2017/bitcoin/dont-trust-yet.png`, visited on 2023-06-06. 52

[128] Bashir, Imran: *Mastering blockchain.* Packt Publishing Ltd, 2017. 52

[129] Sanderson, Grant: *limited-to-2400.png.* `https://3b1b-posts.us-east-1.linodeobjects.com//content/lessons/2017/bitcoin/limited-to-2400.png`, visited on 2023-06-06. 53

[130] Rauchs, Michel and et al.: *The cambridge bitcoin electricity consumption index.* 2021. `https://cbeci.org/`. 54