University of Brasília

Exact Sciences Institute
Computer Science Department

Exploring the Energy Flow Classifier to Identify Fraudulent Cryptocurrency Transactions

Kevin S. Araujo

Dissertation submitted in partial fulfillment of the requirements to Professional Master's Degree in Applied Computing

Adviser
Prof. Dr. Rodrigo Bonifacio de Almeida

Co-advisor
Prof. Dr. Fabiano Cavalcanti Fernandes

Brasília
2023

Ficha Catalográfica de Teses e Dissertações

Está página existe apenas para indicar onde a ficha catalográfica gerada para dissertações de mestrado e teses de doutorado defendidas na UnB. A Biblioteca Central é responsável pela ficha, mais informações nos sítios:

http://www.bce.unb.br
http://www.bce.unb.br/elaboracao-de-fichas-catalograficas-de-teses-e-dissertacoes

Esta página não deve ser inclusa na versão final do texto.

University of Brasília

Exact Sciences Institute
Computer Science Department

Exploring the Energy Flow Classifier to Identify Fraudulent Cryptocurrency Transactions

Kevin S. Araujo

Dissertation submitted in partial fulfillment of the requirements to
Professional Master's Degree in Applied Computing

Prof. Dr. Rodrigo Bonifacio de Almeida (Adviser)
CIC/UnB

Prof. Dr. Luis Paulo Faina Garcia
UnB

Dr. Alberto Cesar Cavalcanti Franca
UFRPE

Prof. Dr. Marcelo Ladeira
Coordinator of Graduate Program in Applied Computing

Brasília, dezembro 12, 2023

Dedicated to

The dedication section is where the writer expresses gratitude or others, normally those who have inspired or assisted them in their research and writing. It is usually the shortest page of an academic paper.

Acknowledgements

Thanks to Google and Wikipedia.

Abstract

Fraudulent cryptocurrency transactions represent an ongoing and significant threat within the digital asset ecosystem, demanding robust detection mechanisms. Identifying such illicit activities is complicated by the complex nature of transaction data and, critically, the prevalent scarcity of labeled illicit examples in available datasets. This paper conducts a comprehensive empirical evaluation of the Energy Flow Classifier (EFC), a physics-inspired one-class anomaly detection model, for identifying illicit Bitcoin transactions using the Elliptic dataset, specifically addressing its performance under conditions of label scarcity. Our findings demonstrate that EFC can effectively distinguish illicit from licit transactions when trained exclusively on normal data, with its performance significantly enhanced by combining feature selection and data balancing techniques like SMOTE, achieving strong results even on imbalanced test sets.

Keywords: criptocurrencies, anomaly detection, machine learning

Contents

List of Figures

Chapter 1

Introduction

Money laundering is a high-impact global problem, with criminals laundering billions of dollars annually from serious felonies. In recent years, cryptocurrencies have emerged as a significant channel for these illicit activities, largely due to the pseudonymity they offer criminals. Machine Learning (ML) presents a powerful tool for identifying the complex patterns associated with such illicit financial flows, potentially increasing detection rates while decreasing the high false-positive rates common in traditional rule-based systems.

However, the practical application of ML in this domain faces a critical obstacle: the scarcity of labeled data. Supervised learning algorithms, which typically offer high accuracy, are often unfeasible because large-scale labeled datasets of illicit transactions do not exist. This label scarcity stems from the evolving complexity of money laundering schemes, which makes identifying all illicit actors nearly impossible, and the fact that acquiring labels from law enforcement or expert manual annotation is a costly and slow process.

Previous research exploring this problem on the Elliptic Bitcoin dataset has shown that traditional unsupervised anomaly detection methods are also inadequate. A key finding is that illicit transactions do not necessarily present as statistical outliers; instead, sophisticated criminals often attempt to mimic normal behavior, effectively hiding their activities within clusters of legitimate transactions. While techniques like Active Learning have been shown to achieve high performance by using a small fraction of labels, this dissertation explores a different approach to contend with the challenge of label scarcity.

This research proposes the application of the Energy-based Flow Classifier (EFC), a novel algorithm initially developed for network intrusion detection systems. The EFC is an anomaly-based classifier that uniquely infers its statistical model based *solely* on benign (or licit) examples. By learning the fundamental properties and correlations within normal traffic, it can classify new, unlabeled instances based on how much they deviate from the established benign model.

The primary advantage of the EFC in the context of money laundering detection is its inherent ability to operate in an environment with a severe lack of illicit labels, as it does not require malicious samples for training. Therefore, this study aims to adapt and apply the EFC algorithm to the Elliptic dataset to evaluate its effectiveness in detecting illicit Bitcoin transactions. We will assess whether the EFC provides a robust and practical alternative to previously studied supervised and unsupervised methods, given its white-box nature and its design for label-scarce scenarios.

Bitcoin is an electronic transaction system that operates without a third-party moderator [1]. It is built on blockchain technology, where an immutable ledger of financial transactions is maintained through mathematics, programming, and advanced cryptography. This distributed ledger architecture eliminates the need for central authorities to establish trust. Although Bitcoin was designed to circumvent vulnerabilities in the traditional financial system [1], it is not immune to manipulation and anomalous activities and demands a robust detection mechanisms [2, 3, 4].

In fact, crypto-related fraud has become a significant threat, causing substantial financial losses and destroying trust in the digital asset ecosystem. In 2023, for example, illicit addresses received \$24.2 billion in cryptocurrency, indicating the scale of financial losses from scams, stolen funds, and other illicit activities [5]. These activities not only cause direct monetary damage to individuals and institutions, but also have broader implications, such as undermining the legitimacy of cryptocurrency markets and hindering the widespread adoption of blockchain technology. The need to develop effective methods for detecting and preventing cryptocurrency fraud is crucial to protect participants, maintain market integrity, and ensure sustainable growth of the cryptocurrency industry [6, 7].

However, detecting anomalous patterns within the intricate data streams of cryptocurrency transactions poses a significant challenge. Like many modern datasets, these transactions are characterized by high dimensionality, evolving characteristics, and substantial volume, which complicates the application of traditional anomaly detection methods. In this context, the Energy-Based Flow Classifier (EFC) presents a promising approach rooted in statistical physics. Originally formulated using the Inverse Potts model [8], the EFC characterizes the probability distribution of normal data flows through an energy function derived from observed data patterns [8]. Previous research has demonstrated the utility of EFC in classifying unusual network traffic, suggesting its potential to adapt to detect fraudulent activity within cryptocurrency systems [8, 9]. Its selection for this study is further motivated by its relatively low computational complexity during both training and inference phases, rendering it a suitable candidate for real-time detection applications where swift identification of illicit activities is paramount.

Building upon the promise of the Energy-Based Flow Classifier (EFC) framework, this paper presents a comprehensive empirical evaluation of its application to the detection of illicit Bitcoin transactions. To this end, we first replicate a previous study that employs machine learning algorithms such as K-Nearest Neighbors, One-Class Support Vector Machine, and Isolation Forest for anomaly detection on the Elliptic dataset [1]. We then investigated the use of EFC as a potential alternative to these machine learning approaches, using the same data set for consistency. Our findings confirm the EFC's ability to distinguish between licit and illicit transaction patterns based on their energy profiles, showing strong performance in identifying illegal activity even when trained solely on licit data. However, the results also highlight the critical sensitivity to specific configuration parameters. In particular, we observe significant trade-offs between maximizing the detection rate of illicit transactions (recall) and minimizing false positives (precision), especially concerning the energy threshold that defines anomalous behavior.

Addressing the significant challenge of label scarcity inherent in datasets like Elliptic is crucial for developing effective fraud detection systems. Traditional supervised machine learning methods often struggle in such scenarios due to the limited availability of labeled illicit examples. This motivates the exploration of alternative approaches, particularly those capable of learning from predominantly normal data. The Energy-based Flow Classifier (EFC) also emerges as a promising candidate in this regard. Originally proposed for network intrusion detection [8, 9], EFC was designed specifically to address key limitations of conventional ML classifiers, including the reliance on extensive labeled datasets. A core strength highlighted in its foundational work is its ability to function as an anomaly-based classifier, inferring a statistical model of normal behavior using only labeled *benign* (or licit, in our context) examples [9]. Deviations from this learned norm, characterized by higher 'energy' scores, are then flagged as potential anomalies. This one-class learning paradigm directly tackles the label scarcity issue prevalent in the Elliptic dataset, allowing us to model legitimate transaction patterns effectively even with few confirmed illicit instances. Furthermore, EFC's demonstrated adaptability across different data distributions in network traffic analysis suggests potential robustness in the dynamic environment of cryptocurrency transactions. Consequently, this paper evaluates the suitability and performance of EFC for identifying illicit Bitcoin transactions by leveraging its capacity to model normality from available licit data.

1.1 Goals

Research Question: *To what extent is the Energy-based Flow Classifier (EFC) a viable and effective alternative to conventional machine learning models for detecting illicit*

[1] Available at https://www.kaggle.com/ellipticco/elliptic-data-set

Bitcoin transactions given the real-world challenge of label scarcity?

- **Main Objective** To empirically evaluate the effectiveness of the Energy Flow Classifier (EFC), a one-class anomaly detection model, for identifying illicit Bitcoin transactions in the Elliptic dataset, particularly under the real-world constraint of label scarcity.

  Specific Objectives:

  - To adapt and apply the Energy Flow Classifier (EFC), a model originally from network intrusion detection, to the domain of cryptocurrency fraud, training it exclusively on licit transaction data to establish a baseline performance on the raw, imbalanced Elliptic dataset.
  - To systematically investigate the impact of various data balancing techniques including undersampling, oversampling, and the Synthetic Minority Over-sampling Technique (SMOTE) on the EFC's ability to classify illicit transactions.
  - To analyze the effect of dimensionality reduction on EFC's performance by applying feature selection (SelectKBest) to identify an optimal subset of features for distinguishing between licit and illicit activity.
  - To assess the performance of a combined strategy that integrates feature selection with data balancing (SMOTE) to determine if this synergistic approach yields superior classification results on a realistic, imbalanced test set.
  - To compare the performance of the optimized EFC configuration against established methodologies from previous work, providing a conclusive answer on its viability as a practical tool for fraud detection in label-scarce cryptocurrency environments.

References

[1] Nakamoto, Satoshi: *Bitcoin: A peer-to-peer electronic cash system.* 2008. `https://bitcoin.org/bitcoin.pdf`. 2, 7, 8, 17, 18, 22, 23, 24

[2] 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. 2, 21

[3] 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

[4] 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

[5] Chainalysis: *The 2024 crypto crime report*, February 2024. `https://go.chainalysis.com/rs/504-JAF-931/images/Crypto-Crime-Report-2024.pdf`, The latest trends in ransomware, scams, hacking, and more. 2

[6] Scharfman, Jason: *The Cryptocurrency and Digital Asset Fraud Casebook, Volume II: DeFi, NFTs, DAOs, Meme Coins, and Other Digital Asset Hacks.* Palgrave Macmillan, 2024. `https://doi.org/10.1007/978-3-031-60836-0`. 2

[7] Khiari, Wided, Azhaar Lajmi, Amira Neffati, and Ahmed El Fahem: *Cryptocurrency fraud and its effects on price volatility in the cryptocurrency market.* Journal of Chinese Economic and Foreign Trade Studies, 2025. `https://www.emerald.com/insight/1754-4408.htm`. 2

[8] Pontes, Camila F. T., João J. C. Gondim, Matt Bishop, and Marcelo Antonio Marotta: *A new method for flow-based network intrusion detection using inverse statistical physics.* CoRR, abs/1910.07266, 2019. `http://arxiv.org/abs/1910.07266`. 2, 3

[9] Souza, Manuela M. C., Camila Pontes, Joao Gondim, Luis P. F. Garcia, Luiz DaSilva, and Marcelo A. Marotta: *A novel open set energy-based flow classifier for network intrusion detection*, 2022. `https://arxiv.org/abs/2109.11224`. 2, 3

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

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

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

Supplement I

Appendix

I.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 [1]. 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.

I.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 [1]. 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 [?]. 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) [1]:

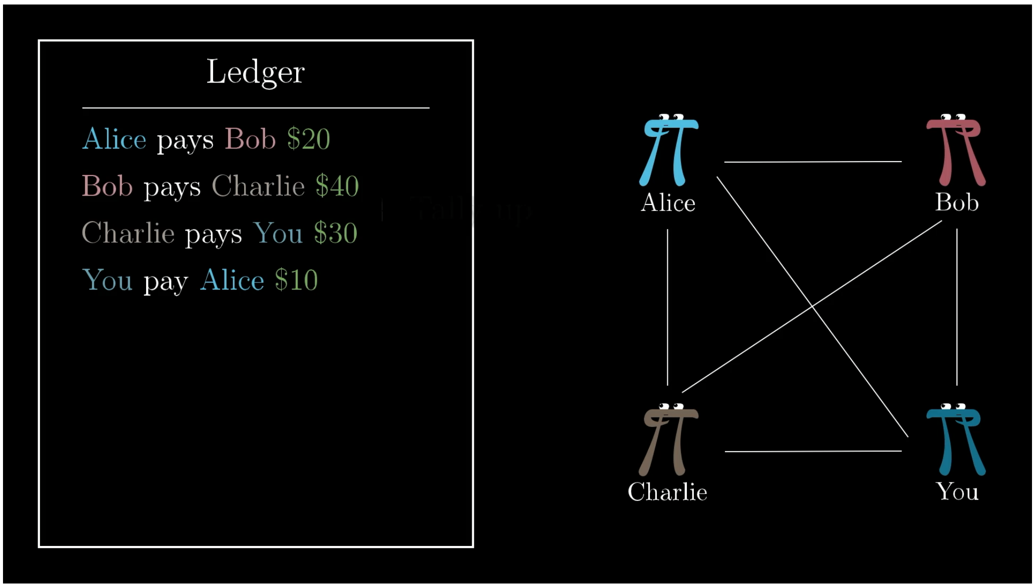
> *the root problem with conventional currencies is all the trust that's required to make it work*

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 [?].

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.



Ledger

Alice pays Bob $20

Bob pays Charlie $40

Charlie pays You $30

You pay Alice $10

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

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.*

I.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 [?].

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 [?]. 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 [?].

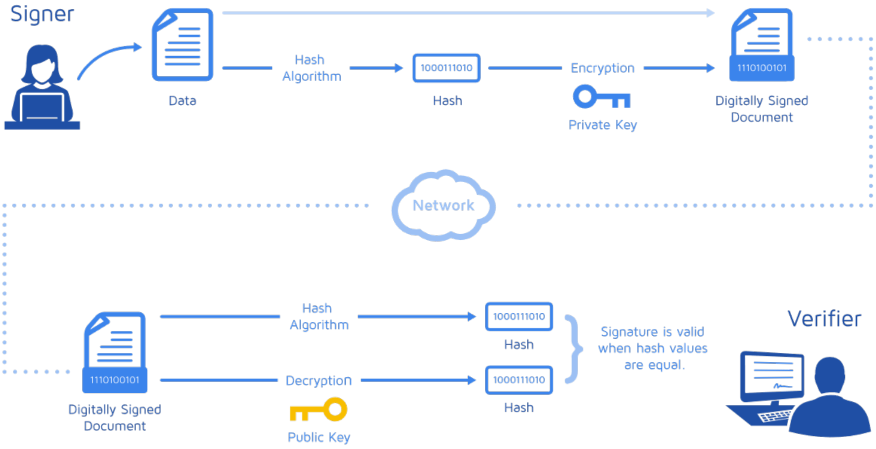


Figure I.2: Digital signature (Reference: [?]).

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 [?]. 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 [?]. 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 [?].

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 [?]. 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 [?]. 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.

I.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 [?]. 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 [?]. 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 [?].

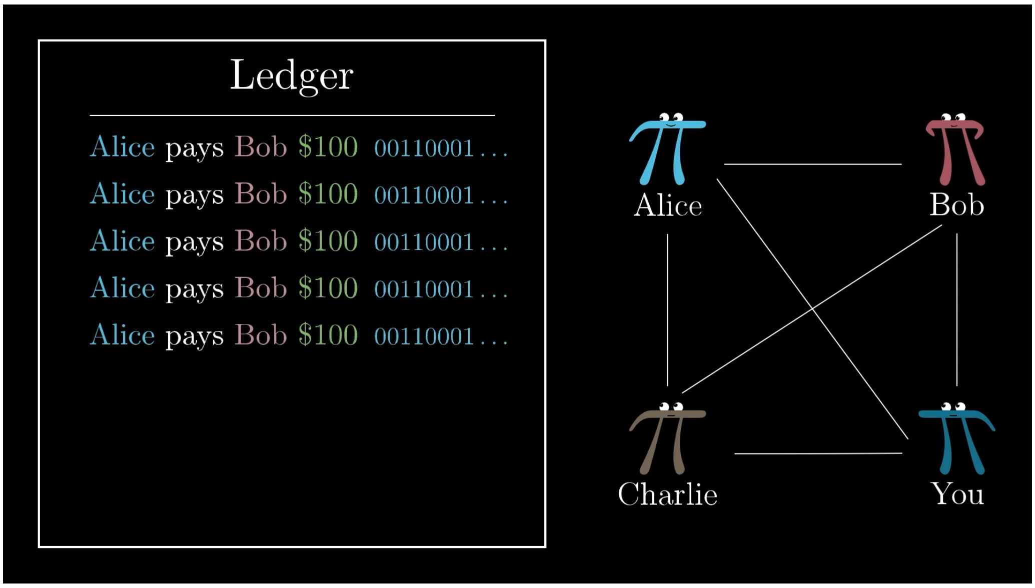

Ledger
Alice pays Bob $100 00110001...
Alice pays Bob $100 00110001...
Alice pays Bob $100 00110001...
Alice pays Bob $100 00110001...
Alice pays Bob $100 00110001...
Alice
Bob
Charlie
You

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

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 [?] 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.

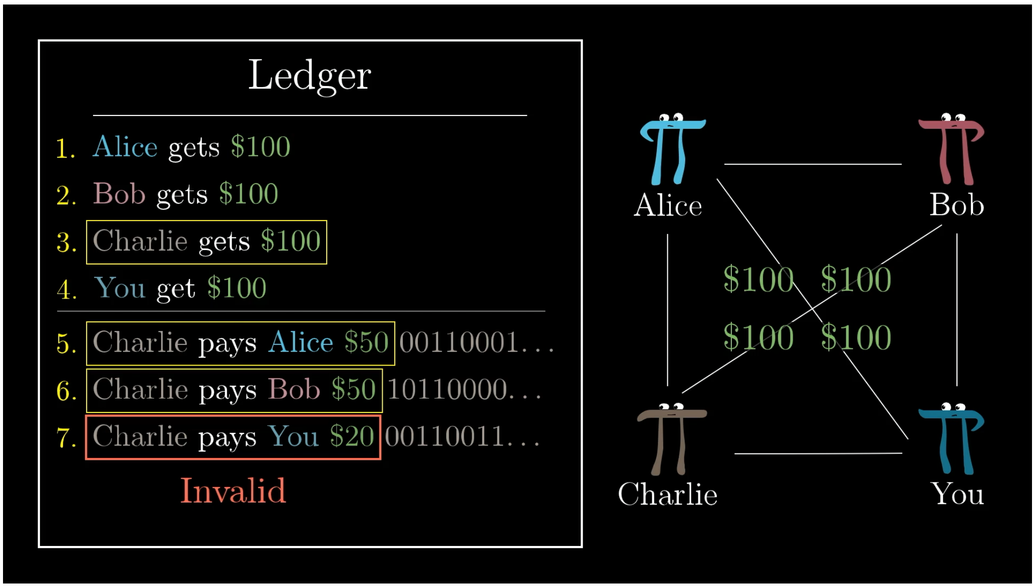
Removing Cash

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

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.

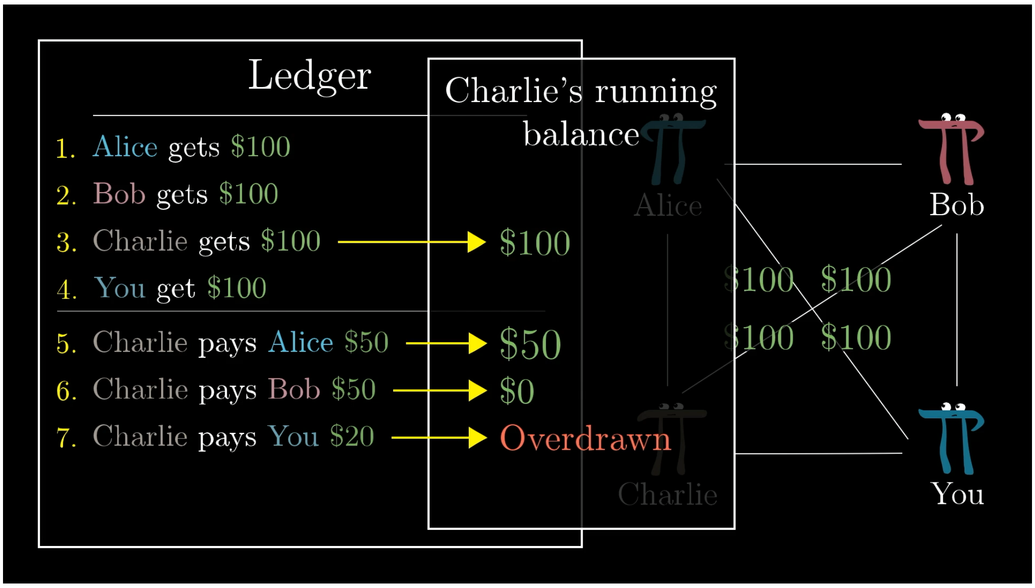


Figure I.5: Now verifying a transaction requires checking the entire ledger history to make sure nobody overdraws. (Reference: [?]).

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

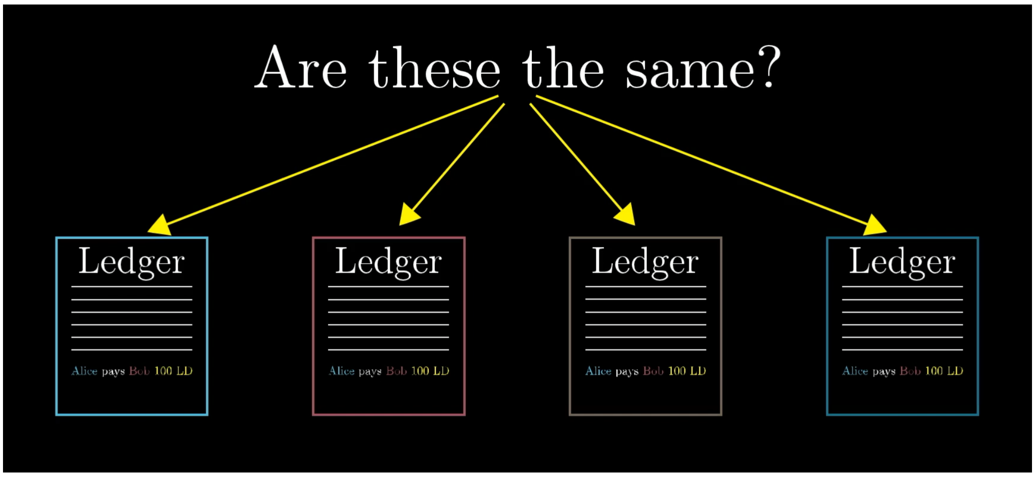


Figure I.6: If everyone keeps a unique copy of the ledger, how can we ensure that everybody agrees on what it should say? (Reference: [?]).

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.

I.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 [?]. This means that it is computationally infeasible to compute the original message from its hash value in reverse direction [?]. Therefore, given a specific hash value such as $1001111100111100\ldots$, 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.*

I.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 [?].

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 [?]. 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 [1].

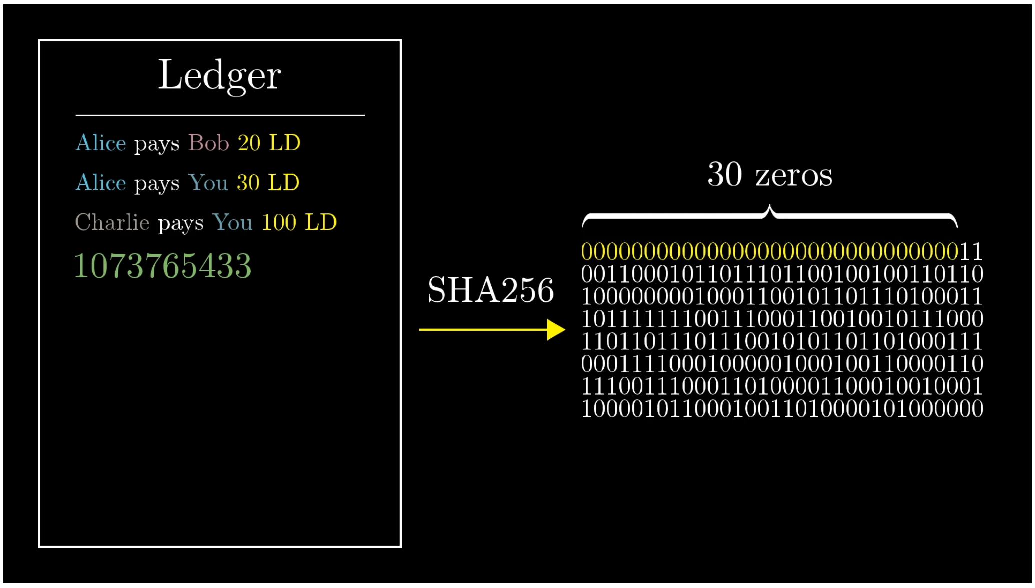


Figure I.7: There is no better way than guess and check for the special hash (Reference: [?]).

I.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 [?].

The core concept of the original Bitcoin paper [1] 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.

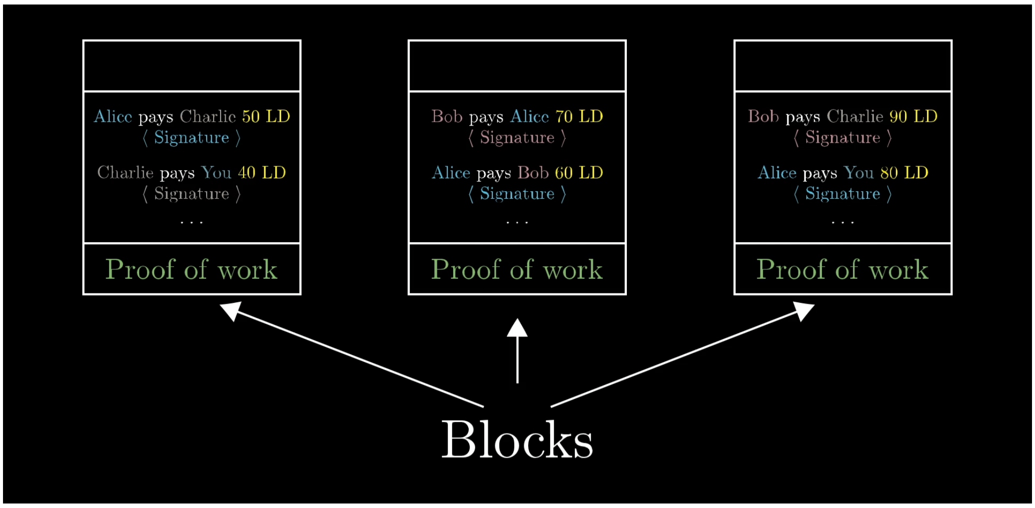


Figure I.8: Blocks on a blockchain (Reference: [?]).

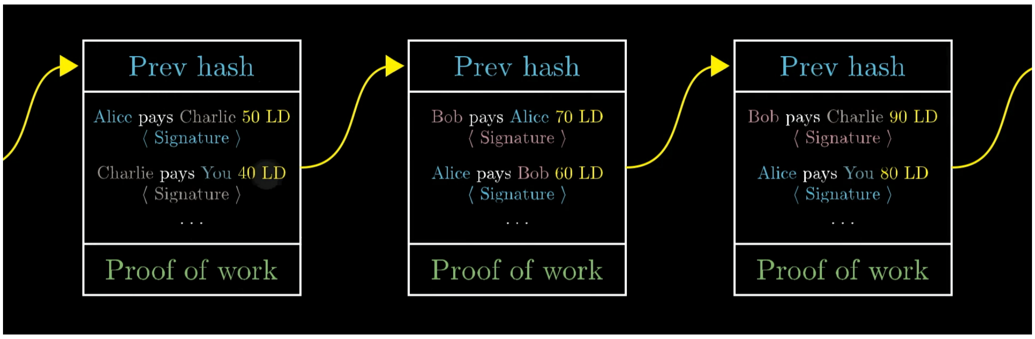


Figure I.9: Because blocks are chained together like this, instead of calling it a ledger, this is commonly called a “blockchain” (Reference: [?]).

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 [?].

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 [?].

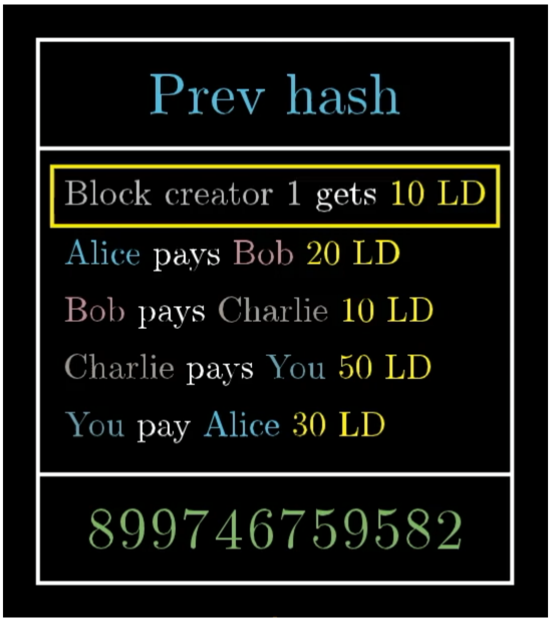


Figure I.10: Block reward (Reference: [?]).

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 [?]. 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) [2].

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 [?]. 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 [1].

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 [?].

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 [?].

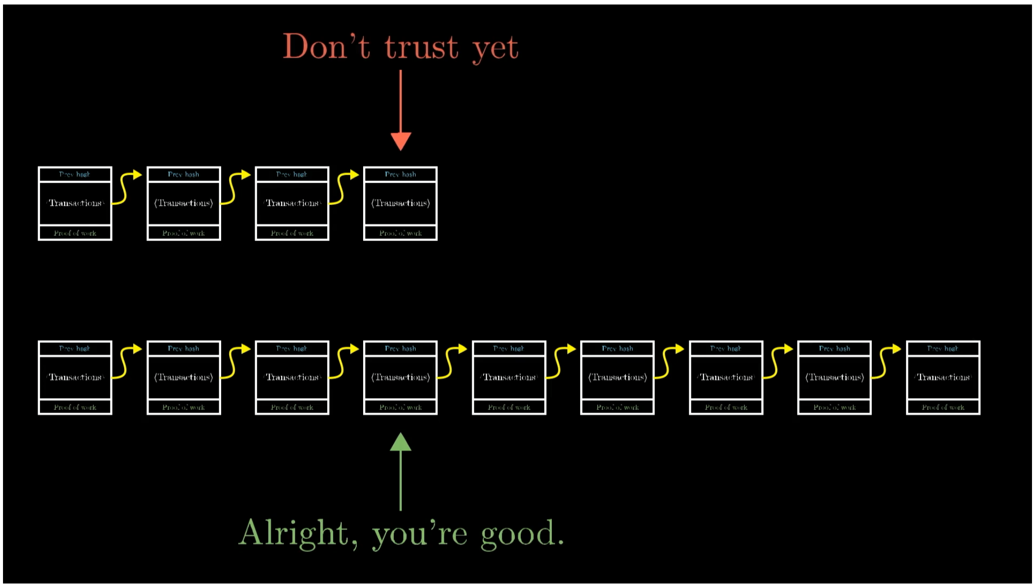


Figure I.11: Blocks are most trustworthy when they aren't brand new (Reference: [?]).

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 [?]. 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 [1].

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 [1]. However, miners can also earn transaction fees by including them in the validation process of transactions.

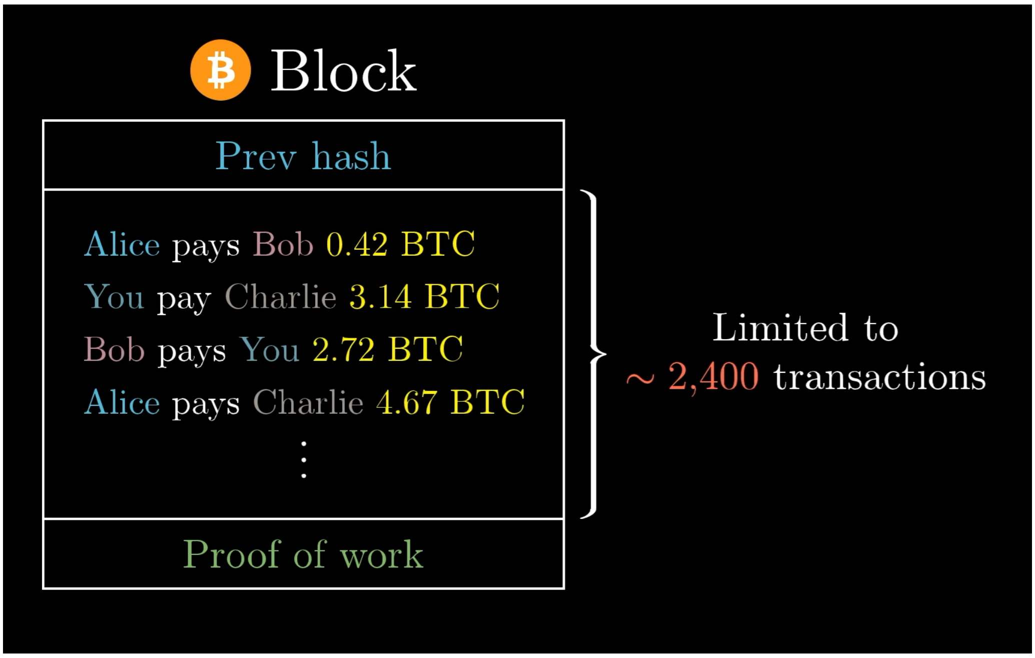


Figure I.12: Transactions on a bitcoin blockchain is limited (Reference: [?]).

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 [?].

I.2 Money is Corruptible

Bitcoin (BTC) emerged on the scene in late 2008, allegedly as a response to the financial crisis of 2007-2008, and some have suggested that it was also motivated by frustrations with the bureaucratic nature of the Japanese banking system. However, the latter claim ventures into more conspiratorial territory; although there is no concrete evidence to support this claim, the original author or authors of the Bitcoin whitepaper may have had connections to Japan [1]. Nevertheless, prior to delving into the intricacies of Bitcoin, it is crucial to first explore the concept of money and, more significantly, its foundational aspect: value. In the following sections, we will focus on the economic concept of money as a store of value and medium of exchange and explore how Bitcoin fits into this framework.

What is Money? Or rather, what does money represent?

I.2.1 What is Money

If we asked: *What is man's greatest invention?* What would your answer be? There are a lot of options. Would it be fire? Because it gives us warmth, protection, and the ability to cook our meals? Or perhaps you would pick the wheel? Because it's the driving force being the beginnings of trade, commerce, and travel. While both of those are excellent choices, most of the time when we think about the greatest inventions of mankind, we tend to forget one of the most important ones of all: money. Unlike tangible inventions such as fire and the wheel, money, possesses an immaterial nature. It exists as a conceptual construct, lacking inherent value, and its significance is derived solely from the subjective importance we attribute to it. This intangible nature of money often distinguishes it from other notable inventions in the collective human consciousness [?].

Notwithstanding the illusory nature of money, its significance remains unaffected. Before to the establishment of monetary systems, human societies engaged in the direct exchange of goods and services, known as the Barter system. In this system, individuals traded commodities without an assigned intrinsic value, relying solely on subjective evaluations of desired items. Consequently, each transaction was contingent upon the willingness of the parties involved to forfeit possessions in pursuit of their desired commodities. Such an exchange mechanism resembled a game-like scenario [?]. If I desired vegetables for my meal but my only possession was cattle, I would be obliged to offer one of my animals in exchange for bags of vegetables. Similarly, if I required footwear but specialized in tent production, I would have to surrender an entire tent to obtain a pair of slippers. This barter-based system reveals a prominent issue known as asymmetry. As a tent-maker, the exchange of an entire dwelling for simple footwear would undoubtedly leave me feeling disadvantaged. The absence of a standardized medium of exchange presented significant challenges for facilitating agreements between individuals with disparate needs. Moreover, the reliance on a fortuitous occurrence of complementary wants, wherein two individuals simultaneously sought reciprocal possession, further complicated matters, rendering the process inefficient [?].

Our monetary system serves not only as a medium of exchange but also as a store of value. However, prior to the advent of money, certain individuals were unable to effectively preserve their wealth, through no fault of their own. Consider the scenario of a farmer selling tomatoes and a tent maker. The tent maker has the ability to amass a substantial portfolio of real estate in the form of tents, which can be bartered year-round with individuals in need of shelter. Consequently, the tent maker has the opportunity to accumulate wealth. In contrast, the farmer selling tomatoes can only engage in barter transactions during the tomato season. Moreover, due to the perishable nature of tomatoes, long-term storage is not feasible. Thus, despite exerting comparable efforts in their respective businesses, the farmer had no viable means to sustain wealth throughout the year [?]. There's also the problem of having something that only a very few people want. Nowadays, when starting a business, you're often told to find a niche. A small group of people who are very interested in what you have to offer. Before money was a thing, that advice would have left you with nothing worth bartering.

In societies where possessions in high demand, such as weapons, animal skins, and salt, held significant value, individuals who possessed such commodities acquired substantial wealth. The awareness that these items were universally sought-after prompted individuals to engage in anticipatory buying, even if immediate need was absent, to secure future trading opportunities. As a consequence, the emergence of commodity money ensued, whereby goods and services were exchanged for commonly recognized items such as salt or weapons, facilitating subsequent transactions with other parties [?].

Humanity progressed beyond direct barter, encompassing a diverse range of commodities including salt, weapons, and minutecollectibles like shells and beads. This evolution introduced a more efficient method of trade and exchange. Rather than directly swapping goods and services, individuals adopted the practice of using arbitrary objects as intermediary placeholders of value, effectively functioning as IOUs (I Owe You). Subsequently, these placeholders could be utilized to acquire desired goods and services from others. This concept proved remarkably ingenious, ultimately leading to a global transition from the Barter system to the monetary exchange system [?]. However, there has been a persistent limitation associated with this form of exchange. In order for currency to exhibit intrinsic value, it requires a degree of scarcity [?, ?]. The more easily accessible an item is, the lower its perceived worth [?]. When an item is readily obtainable by anyone, its value diminishes considerably. As a result, substances such as sand or shells, which can be effortlessly collected from any beach, do not effectively function as indicators of value [?, ?].

In approximately 770 BC, China witnessed the emergence of the earliest metal coins, marking a significant milestone in the evolution of currency. As a tribute to their historical currency systems, the Chinese craftsmen ingeniously crafted miniature replicas of tools that were previously utilized as forms of exchange. To ensure convenient handling, the coins were deliberately designed in a circular shape, allowing easy retrieval from pockets without causing any discomfort to the fingers. These coins were predominantly cast using bronze, thereby bestowing intrinsic value upon them. This transition marked a pivotal moment in history, as money transformed from a mere symbol to a tangible entity of worth. The scarcity of bronze, a resource not readily available on any beach, further amplified the significance of these coins [?, ?]. During this period, the concept of money had not yet deviated from material reality. The valuation of a coin corresponded directly to the intrinsic value of the metal constituting the coin. For instance, a coin crafted from 1 gram of gold possessed an equivalent worth of precisely 1 gram of gold. This quantifiable attribute allowed for straightforward verification through direct measurement, enabling individuals to visually ascertain that the coin indeed comprised 1 gram of gold.

The realization of the potential power of money was swift among Kings and Rulers [?]. This understanding led to the creation of the first official money mint by Alyattes, the King of Lydia, around 600 BC. These coins were minted from a blend of silver and gold, with each coin featuring a distinctive image serving as a denomination. Consequently, individuals could effortlessly determine the value of their metal possession by observing the pictorial representation on the coin's surface [?]. The pursuit of greater wealth among Kings led to the devaluation of coins through the reduction of precious metal content and the inclusion of cheaper metals [?]. This resulted in the divergence between the face value and actual worth of circulating coins, establishing the illusion of money. The value of coins became divorced from the intrinsic value of their metal composition, relying instead on the dictates of rulers and financial institutions [?]. As an example, the British Pound Sterling ceased to represent a fixed quantity of Sterling Silver and instead denoted a unit of currency determined by authoritative decree.

The emergence of international trade exposed the impracticality of metal coins, leading to the introduction of IOU certificates by the Kings to facilitate long-distance transactions [?]. These certificates, bearing the King's stamp, gained trust and were believed to hold value, as they were expected to be exchangeable for equivalent coins. Initially, this belief corresponded to reality. With the proliferation of IOU certificates in circulation, the necessity for physical coins diminished. Ultimately, the value of the certificates became divorced from their direct convertibility into gold and silver coins. Instead, their value relied on collective trust and shared belief [**?**]. This shift allowed the paper certificates to retain value based on our perception, even in the absence of an immediate exchange for tangible precious metals.

I.2.2 The Illusion of Money

From Ancient Kings to modern-day governments and Central Banks, money has remained an illusion. A mere representation of whose value is determined by the importance people place on it.

The ten thousand Singapore Dollars banknote, while no longer in production, remains the highest denomination in circulation [**?**]. Despite its intrinsic production cost of fewer than 20 cents, the value of this paper note is upheld by the illusion perpetuated by the fiat currency system [**?**]. Presently, its monetary equivalence to seven thousand three hundred and forty-five US Dollars enables its utilization in acquiring substantial assets such as houses, cars, and even valuable commodities like gold.

"Fiat" is the fancy word we use to describe the modern-day illusion. It's a Latin word that translates to "let it be done." It's a decree by the government that, in the case of money, determines what its value is and enforces it as legal tender [**?**, **?**].

The elusive nature of money often evades careful consideration, yet akin to historical rulers, contemporary governments possess an understanding of the influential power of currency and persistently strive for its accumulation. Recognizing that the possession of greater quantities of these paper instruments equates to amplified authority, governments adopt the approach of generating additional currency ex nihilo. For instance, in the scenario where the United States government necessitates $340 million dollars to procure an F-22 jet, it possesses the capacity to create the required funds through the act of monetary printing [**?**, **?**]. But there is one problem with this: **inflation**.

The fundamental attribute of money lies in its role as a medium of exchange, conferring value upon it [**?**]. Consequently, the quantity of money in circulation should align with the aggregate production of goods and services. Should the issuance of money exceeds the availability of goods and services, with all else remaining constant, the resultant effect is an escalation in prices and a subsequent devaluation of the currency itself. This concern resonates with economists and the general population, including individuals such as ourselves, [**?**], particularly in the context of the current global reserve currency, the United States Dollar.

The year 2020 proved to be an exceedingly challenging period for the world at large, as the onset of the pandemic necessitated the temporary closure of numerous economies, resulting in a considerable reduction in the availability of goods and services and a marked decline in overall economic output, as outlined in the World Economic Outlook report by the International Monetary Fund [?]. To avert economic collapse and the potential disintegration of societal systems, the US government embarked on an unprecedented scale of monetary expansion, surpassing any previous instances of currency printing in its history [?]. As of 2021, the current state of affairs reveals a considerable expansion of the US dollar supply, with approximately 40% of the existing currency having been printed within the last 18 months [?]. This substantial increase in the money supply with the country's output has raised concerns regarding the potential for significant price inflation [?]. Observable evidence of this trend is already apparent in the substantial rise in commodity prices, such as the tripling of lumber prices compared to a year ago. Additionally, discernible price increases can be observed in everyday experiences, including slight increments in prices at favorite restaurants, such as a modest 20-cent rise in the cost of guacamole at Chipotle [?]. Although the provision of stimulus and unemployment checks by governments to their citizens may initially appear beneficial, it entails a double-edged sword. While it undoubtedly assists individuals in dire economic circumstances, it also introduces challenges. Presently, the combined factors of inflationary pressures and an economic slowdown have created difficulties for individuals seeking suitable employment opportunities, not solely due to a lack of willingness but also because certain job options may be less desirable than available alternatives [?, ?].

An illustrative example can be observed in the United States, where the law does not mandate a minimum wage for individuals working as waiters or waitresses [?]. Consequently, some employees in these roles receive meager hourly wages, such as $2 to $3, with tips constituting a substantial portion of their earnings. However, due to the implementation of various restrictions and regulations nationwide, coupled with a decrease in customer traffic, there has been a reduction in both customer volume and disposable income, thereby leading to a decline in tip revenue [?]. Inadequate income for employees may result in higher turnover rates as financial needs are not being met. This situation poses a significant risk to businesses, as the lack of a sufficient workforce can ultimately lead to business closure, setting in motion a cascading effect [?]. A valid concern arises regarding the motivation to actively seek employment when the potential income from unemployment and stimulus checks surpasses that from being employed. This circumstance prompts an examination of the available options. Notably, the Federal Reserve of the United States employs a strategic approach to injecting funds into the economy, a process that may not be widely acknowledged, thus stimulating economic activity without substantial public scrutiny [?]. Consequently, the relative attractiveness of alternative income sources may influence individual's decision-making regarding employment prospects [?].

The United States had accumulated a staggering national debt of $29 trillion before 2020, an astounding and challenging figure to comprehend [?]. This debt is primarily financed through the issuance of bonds and Treasury notes, which are essentially contractual instruments offering repayment of a predetermined principal sum alongside interest [?]. Presently, investing in a 10-year U.S. Treasury bond would yield a modest return of 1.23% upon maturity. Therefore, investing $1,000 today would result in a nominal return of a mere $12.30 by 2031. However, this return fails to keep pace with the targeted inflation rate, projected to be around 2% annually [?]. It should be noted that actual inflation rates may surpass the target, although that discussion is beyond the scope of the current context. Consequently, investing in government notes issued by one's own country, whose currency is utilized in daily transactions, leads to a gradual erosion of purchasing power over a decade. Irrespective of these concerns, financial institutions, businesses, and individuals worldwide participate in the acquisition of bonds and treasury notes, thereby providing governments with discretionary funds for utilization [?]. However, when the government confronts the need to fulfill its debt obligations, the previously obtained funds have been fully expended. Consequently, the government initiates repurchases of treasuries and bonds, confining such transactions to prominent financial institutions and remunerating them through freshly created money, effectively conjured from nothingness. The Federal Reserve, for instance, has repurchased over $1 trillion in bonds since March 2020, with plans to persist in such actions well into the future [?].

Through government injections, banks are empowered to expand their lending activities, thereby increasing interest income and fostering economic growth [?]. However, this surge in lending simultaneously expands the aggregate money supply, leading to a depreciation in the value of each dollar. The implementation of multi-trillion dollar stimulus payments and infrastructure packages raises questions regarding the sustainability of such practices. The influx of new money results in a devaluation of existing money, whereby the balance in an individual's bank account remains unchanged, yet its purchasing power diminishes owing to the influx of newly minted money [?]. Consequently, the retention of wealth in a fiat currency like the US dollar progressively erodes its value, ultimately impeding the ability to acquire goods and services despite nominal bank balances.

The reality that money is nothing but an illusion is one that we must all embrace. Only then will the path to financial freedom become clearer. Understanding that money does not have any intrinsic value in itself but instead only inherits the value we give it.

As the money supply continues to expand, the purchasing power of each dollar held in one's possession inevitably erodes, whereas the dollar-denominated value of global assets tends to appreciate [**?**]. Nevertheless, this perceived growth can be likened to an optical illusion, employing deceptive mechanisms. Despite the seemingly unrelenting ascent of the stock market, the underlying reality is far from reassuring. The relentless depreciation of the currency compounds the situation, eroding its value daily. For example, if the Dow Jones Industrial Average, which serves as a benchmark for the performance of 30 major US companies, were denominated in terms of gold rather than USD, it would become apparent that its value has essentially stagnated since 1997 [**?**].

But what's the end goal of all of this? With fiat and an unlimited supply of money, will the value of each currency just continue to decrease until the end of time? Will the gap between the rich and the poor continue to grow wider? Or are we going to finally fix a problem as old as man itself and stop placing our financial success in the hands of those who are destroying it day by day? Money is corruptible.

Only time will tell, but just to know, there is a way out: **Bitcoin**.