# Blockchain and Digital Money

Zichao Yang

Zhongnan University of Economics & Law

Date: September 2, 2025

# Textbooks

1. Andreas M. Antonopoulos, David A. Harding. *Mastering Bitcoin: Programming the Open Blockchain*. O'Reilly Media, 2023. (Oline Version)

2. Andreas M. Antonopoulos, Gavin Wood. *Mastering Ethereum: Building Smart Contracts and DApps*. O'Reilly Media, 2018. (Oline Version)

3. Andreas M. Antonopoulos, Olaoluwa Osuntokun, Rene Pickhardt. *Mastering the Lightning Network: A Second Layer Blockchain Protocol for Instant Bitcoin Payments*. O'Reilly Media, 2022. (Oline Version)

# Textbooks

4. Fabian Schar, Aleksander Berentsen. *Bitcoin, Blockchain, and Cryptoassets: A Comprehensive Introduction*. The MIT Press, 2020.

5. Lorne Lantz, Daniel Cawrey. *Mastering Blockchain: Unlocking the Power of Cryptocurrencies, Smart Contracts, and Decentralized Applications*. O'Reilly Media, 2020.

6. Jimmy Song. *Programming Bitcoin: Learn How to Program Bitcoin from Scratch*. O'Reilly Media, 2019.

# Class Requirements

- A functional laptop
- Attend the class and participate in discussions
- Pop Quizzes
- Present a group project, 2-3 people per group
- Final report

# I. Introduction: Monetary Theory

# What is Money?

Kocherlakota(1998) described **money** as **memory**.

This definition stems from the observation that people do each other favors on a daily basis without being reciprocated (i.e., *gift-giving* relationships). And for a system of *gift-giving* to function, we need a mechanism for *reaching consensus*.

The *gift-giving* works in a small group where agreement can be reached through negotiations among participants.

In a large group where participants are **anonymous**, *gift-giving* is replaced by the exchange of money. Money keeps an account of the global trade in favors. Money is *memory*.

# Origin of Monetary Unit

Menger(1989) proposed that a monetary unit emerges **spontaneously** from a process in which a good that is frequently traded incrementally becomes a generally accepted **medium of exchange**.

- Money may evolve without government intervention.
- Money shows strong network effects.

In different regions and eras, various items have been used as money (e.g., basic foodstuff, jewelry, precious metals...)

# Functions of a Monetary Unit

Monetary units fulfill three functions: (1) medium of exchange, (2) unit of account, (3) store of wealth.

(1) *medium of exchange*: monetary units can facilitate trade and improve the allocation of goods and services.

(2) *unit of account*: monetary units serve as a universal reference and simplify the comparative valuation of goods and services.

(3) *store of wealth*: monetary units can be used to save.

# Functions of a Monetary Unit

(1) medium of exchange

In an economy that does not use money, goods and services can only be bought through barter.

A barter transaction can only be concluded if one party has what the other party wants and vice versa. This problem is called the *double coincidence of wants*. It is difficult to find a suitable trade partner in a barter economy.

# Functions of a Monetary Unit

## (1) Medium of Exchange

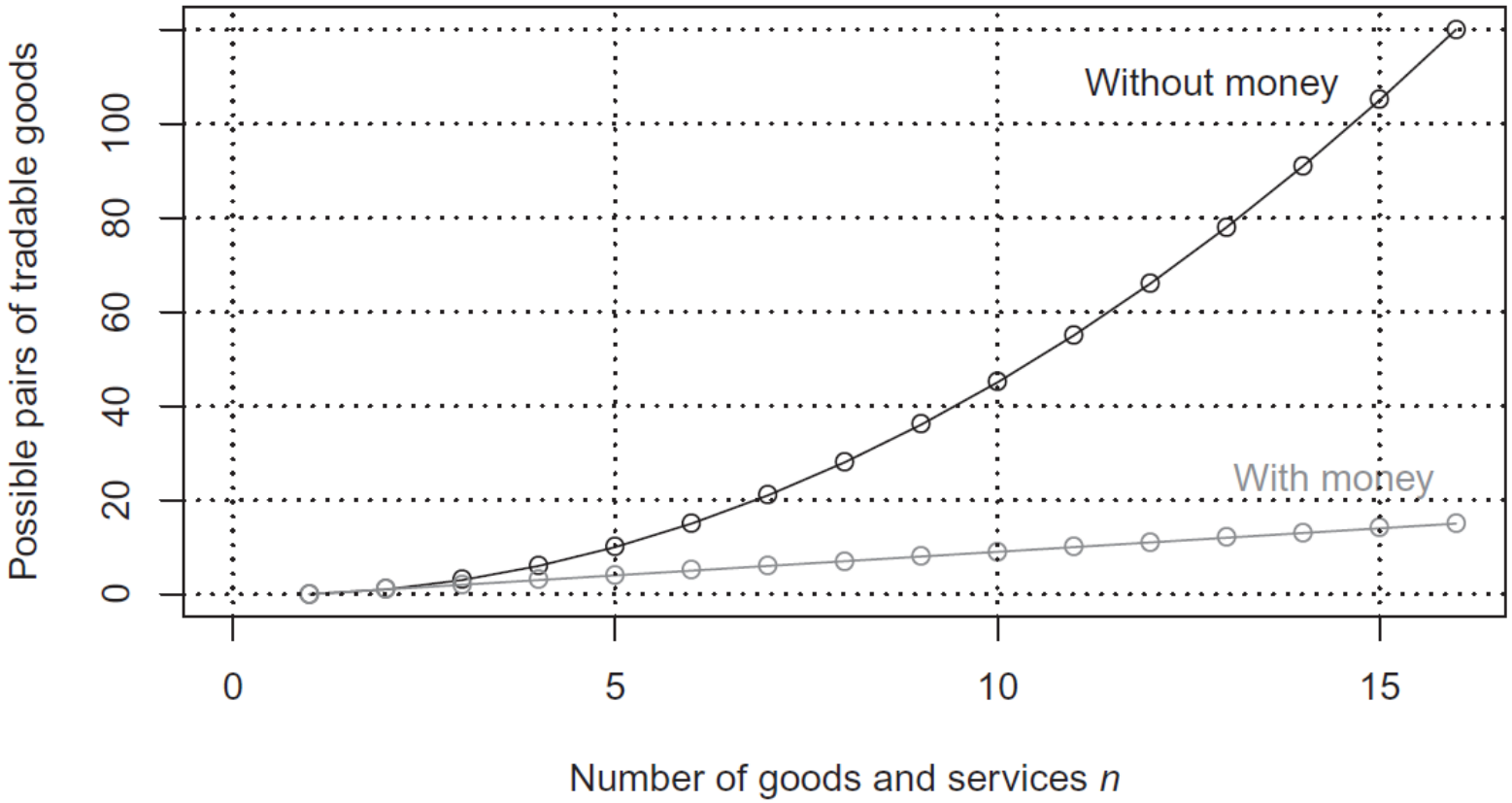



**Figure 1.2**

Number of pairs of tradable goods with and without monetary units.

Source: Fabian Schar, Aleksander Berentsen. *Bitcoin, Blockchain, and Cryptoassets: A Comprehensive Introduction.* The MIT Press, 2020.

# Functions of a Monetary Unit

(2) Unit of Account

A unit of account provides a universal reference for evaluating different types of goods and services. The amount of information required for a comprehensive overview of the market is thereby substantially reduced. ($\frac{n(n-1)}{2}$ pairs of tradable goods to $n-1$ pairs)

**Q**: can multiple monetary units co-exist?

During 1793-1861, approximately 1,600 private banks were permitted to print and circulate their own paper currency in the US. Eventually, 7,000 varieties of these "state bank notes" were put in circulation, each carrying a different design! (Source)

# Functions of a Monetary Unit

(3) Store of Value

A medium of exchange is always a store of value because there is an interval of time between receiving money and spending it.

This function permits consumption smoothing and protection against unexpected expenses.

Assets that can be used as the store of value are not necessarily mediums of exchange, such as real estate or gold.

# Fundamental Properties of Money

To fulfill the above three functions of money, monetary units must be storable, transferable, divisible, homogeneous, verifiable, scarce, and price stable.

- **Storability**: The monetary unit's use as a medium of exchange and a store of value is conditional upon its storability. Goods that are difficult to store are not suitable.
- **Transferability**: It must be possible to transfer the property rights without substantial impediments or costs.
- **Divisibility**: The monetary unit should be able to be exchanged for any chosen quantity of goods or services.

# Fundamental Properties of Money

- **Homogeneity**: Monetary units must be homogeneous; that is, fungible and exchangeable.
- **Verifiability**: The authenticity of the units should be able to be verified and potential counterfeits identified.
- **Scarcity**: If a monetary unit is available in unlimited quantities, it will have no value.
- **Stability of value**: Goods with high seasonal and random supply fluctuations are not suitable.

# Fundamental Properties of Money

**Discussion**: among the following goods, which of them do you think can be used as monetary units?

Stones, shells, cigarettes, grains, fruits, water, oil, jade, gold or real estate?

Figure 1: Rai Stones in Yap island

# Monetary Value

The market value of a monetary unit is based on three components: (1) the intrinsic value, (2) the value of an attached promise of payment, and (3) a liquidity premium.

The **intrinsic value** relates to the material, inherent value of the object.

A **promise of payment** is a component of the value of a monetary unit and it is subject to the issuer risk.

The **liquidity premium** is the outcome of the option to flexibly trade the monetary unit for goods and services.

Now we examine three different types of money based on these three components.

# Money Type: Commodity Money

Commodity money is money whose value comes from a commodity of which it is made. Commodity money has an **intrinsic value** and often contains a liquidity premium.

Examples of commodity money: gold, silver, diamond, salt, tea, alcoholic beverages...


Source: Once Upon a Time in America (1984)

# Money Type: Credit Money

Credit money is a promise of payment and possesses **no intrinsic value**. Generally, it is a piece of paper or a digital record which states that the issuer will make a payment at a specific future date (i.e., IOU).

**Discussion**: One type of credit money is bank deposits:

(1) What are the differences between bank deposits and government-issued money?

(2) What measures have been implemented to address these differences?

# Money Type: Credit Money

**Discussion**: One type of credit money is bank deposits:

(1) What are the differences between bank deposits and government-issued money?

(2) What measures have been implemented to address these differences?



中国人民银行授权使用

# Money Type: Fiat Money

Fiat money is typically designated by the issuing **government** to be legal tender, and is authorized by government regulation.

The expression "fiat money" derives from the Latin term *fiat* (let there be), illustrating that its value has no fundamental basis: it arises out of nothing (let there be money).

The stability of the fiat currency's value is guaranteed uniquely by the central banks, which have an exclusive right to issue the currency and the legal duty to ensure its value remains stable.

# Money Types

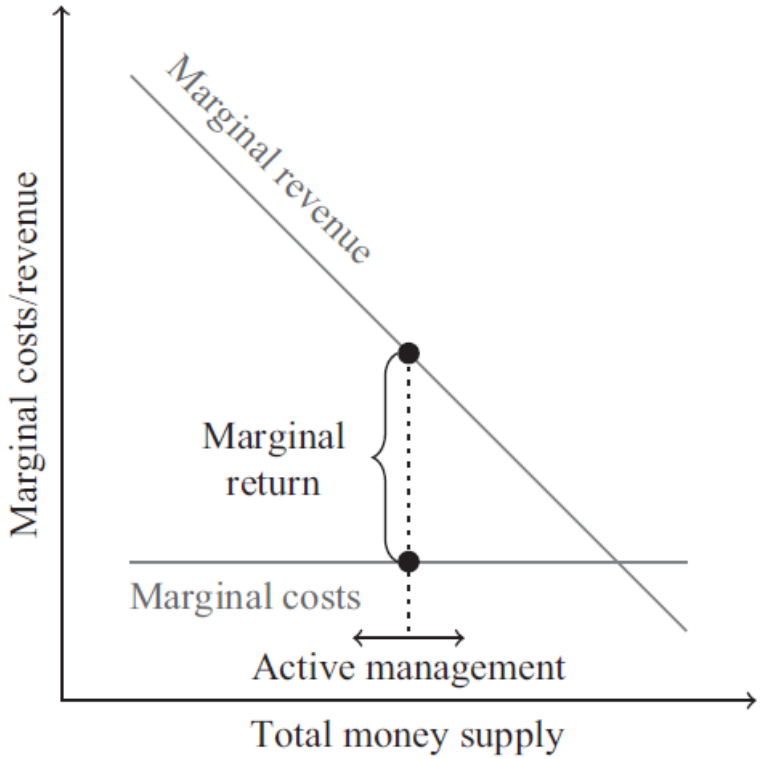
Types of money according to value components.

| | Intrinsic | Promise | Premium |
|---|---|---|---|
| Commodity money | + | | (+) |
| Credit money | | + | (+) |
| Fiat money | | | + |

Source: Fabian Schar, Aleksander Berentsen. *Bitcoin, Blockchain, and Cryptoassets: A Comprehensive Introduction.* The MIT Press, 2020.

# Money Creation

The marginal cost of producing the fiat money is small, and for this reason, a high degree of trust must be placed in the monopoly supplier of money, commonly, the central bank.




Source: Fabian Schar, Aleksander Berentsen. *Bitcoin, Blockchain, and Cryptoassets: A Comprehensive Introduction*. The MIT Press, 2020.

# Money Creation

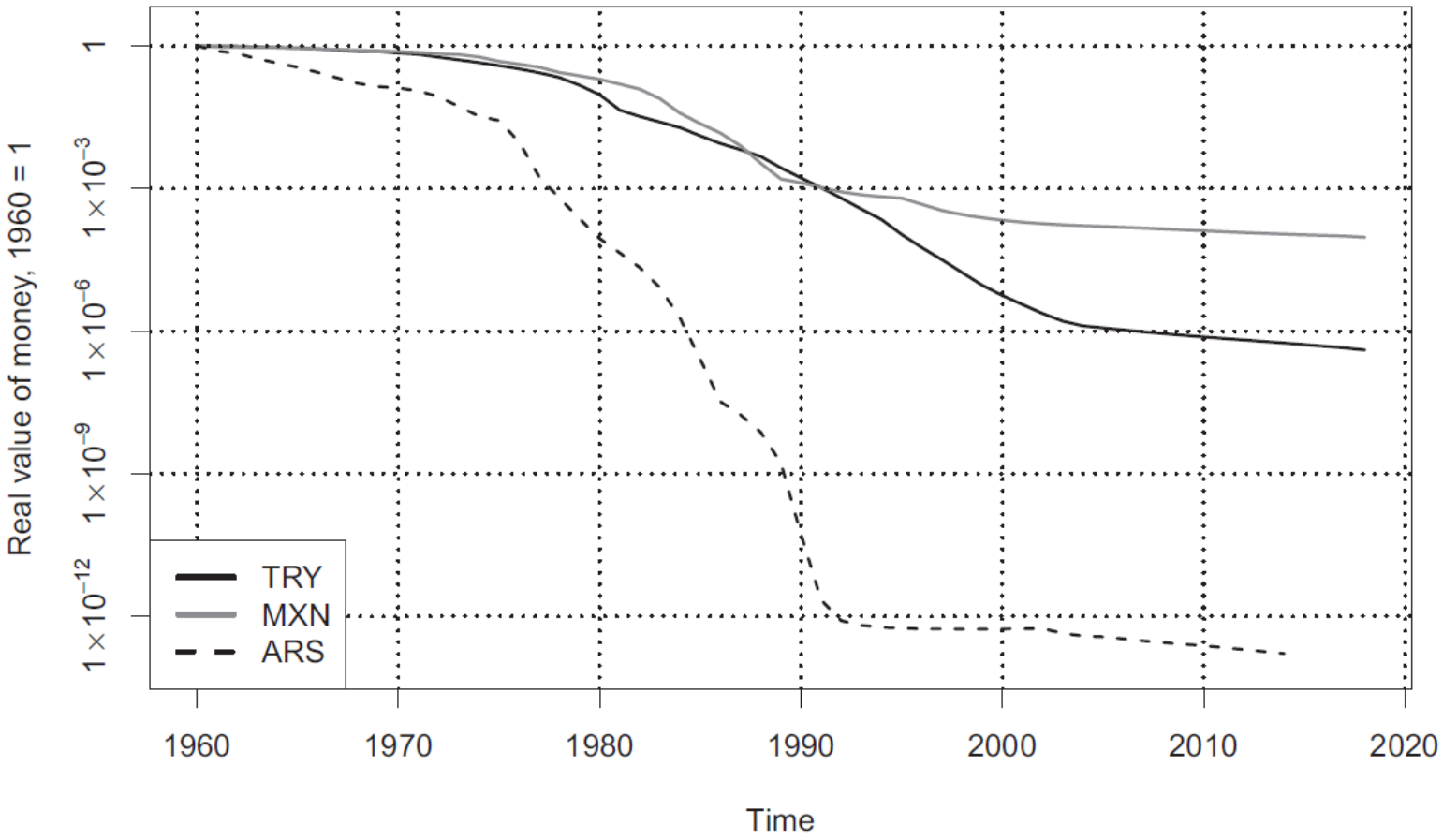



**Figure 1.5**

Development of the real value of money of the Argentine peso, the Mexican peso, and the Turkish lira. Logarithmic scale, normalized to one in January 1960.

*Source*: FRED Economic Data.

# Money Creation

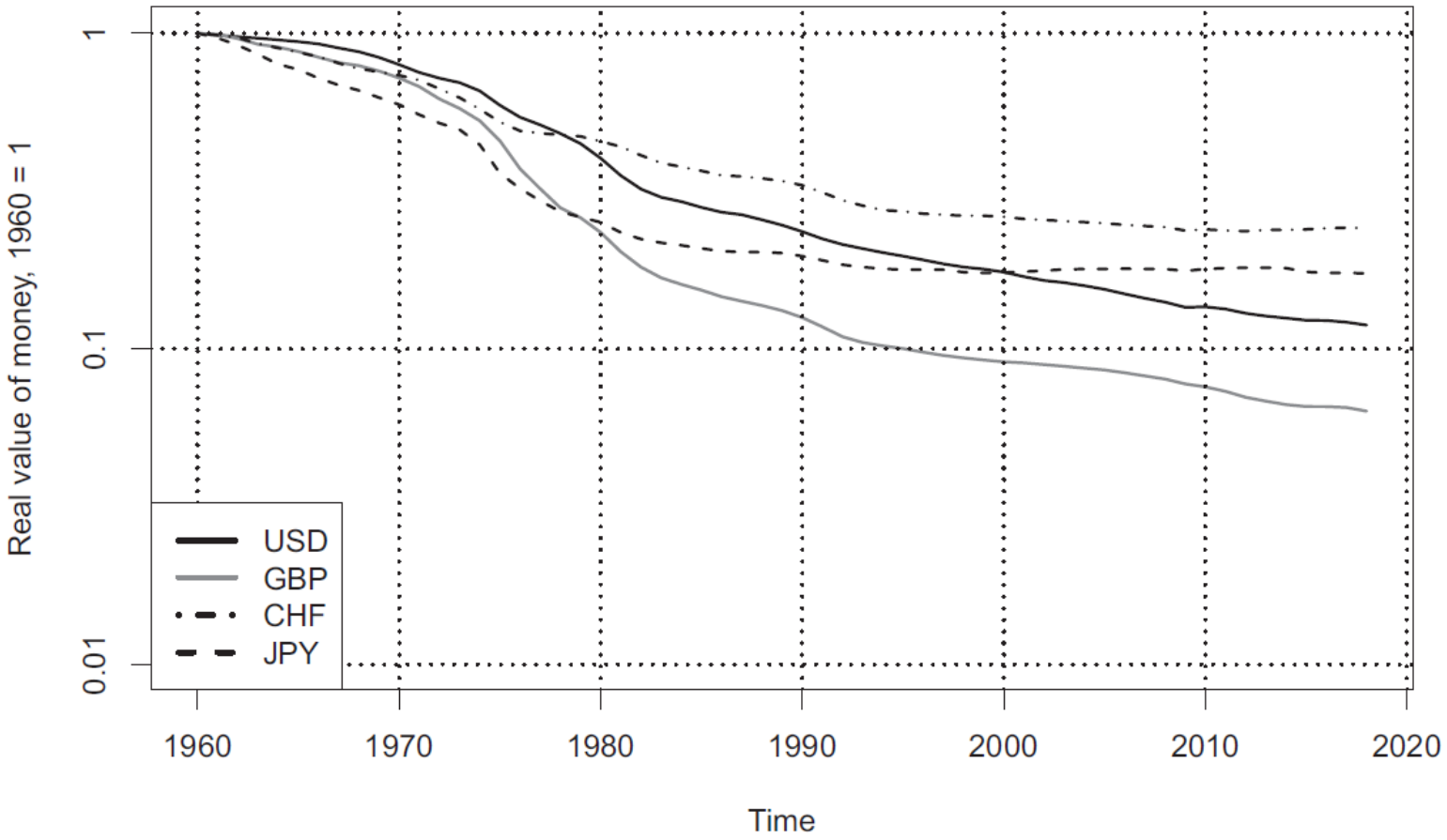



**Figure 1.6**

Development of the real value of money of the US dollar, the British pound, the Swiss franc, and the Japanese yen. Logarithmic scale normalized to one in January 1960.

*Source*: FRED Economic Data.

# Money Creation

**Discussion**:

(1) Why is hyperinflation harmful?

(2) How do people react to hyperinflation? (e.g., Zimbabwe, El Salvador...)

# Money Representation

There are two ways that money can be represented: (1) physical representation, (2) virtual representation.

**Physical monetary units** are linked to an object. The physical control of the object also implies possession of the corresponding value.

**Virtual monetary units** can be transferred to a new owner without the transfer involving a change in control over a physical object.

# Money Representation: Physical Monetary Units

**Advantage**: The ownership rights to physical monetary units are always clearly defined without anyone having to keep records.

This feature allows for a decentralized payment system where physical monetary units can change hands between agents without the involvement of **a third party**.

Therefore, physical monetary units allow agents to **remain anonymous** and protect the owner **against systemic dependencies**.

# Money Representation: Physical Monetary Units

Physical monetary units also have some **disadvantages**:

(1) restricted to a geographic location

(2) generates costs of safekeeping and transport

(3) the monetary unit must be resistant to forgery

(4) dividing a physical monetary unit can be expensive (precious metals) or impossible (banknotes)

# Money Representation: Virtual Monetary Units

Virtual monetary units can avoid all the above disadvantages, but the ownership of a virtual claim is contestable.

To counteract this problem, the legitimization and proof of virtual claims takes place via **implicit or explicit ledgers** that keep a record of all economic subjects' holdings.

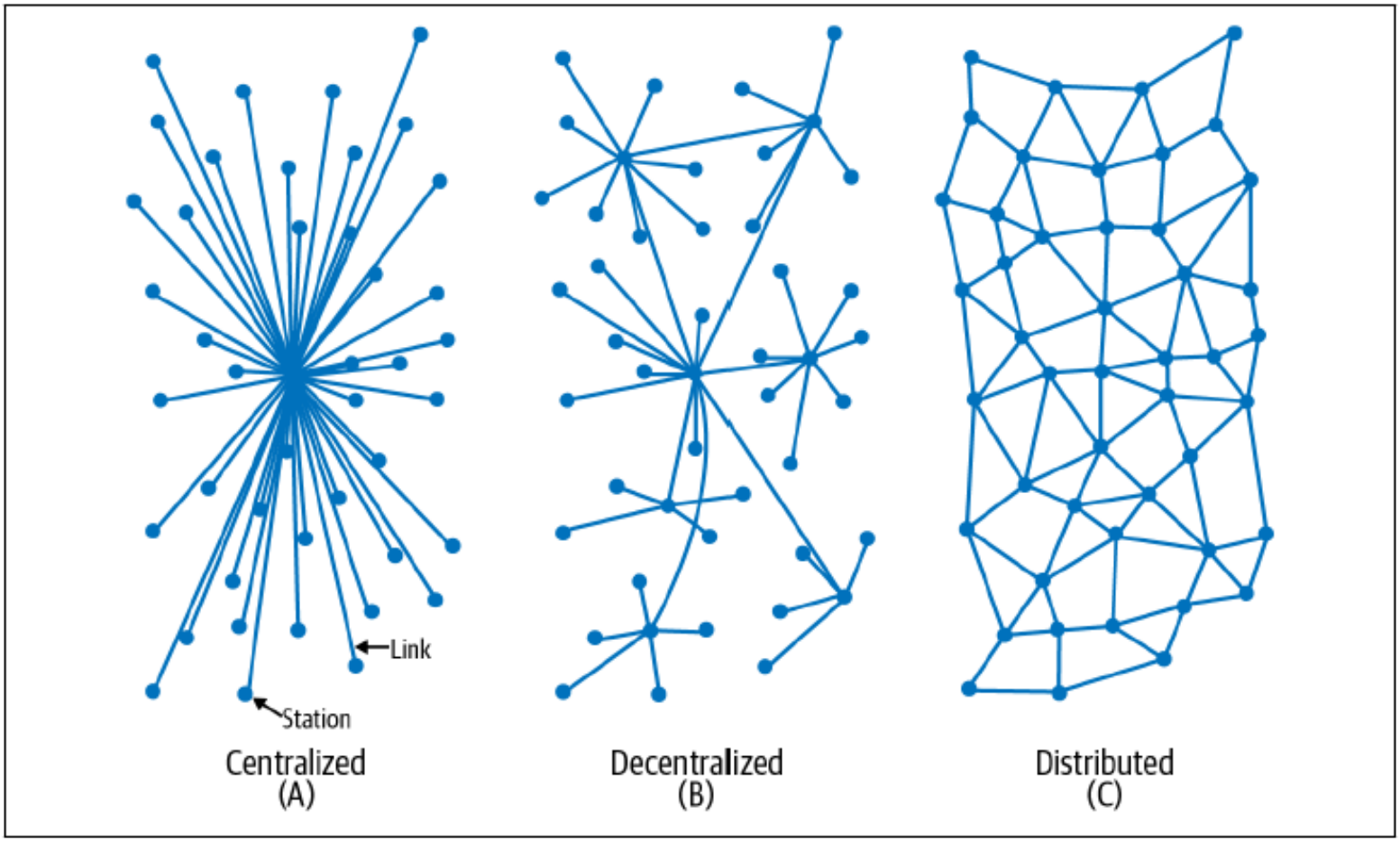
# Ledgers

**Implicit ledgers** are solely based on the oral agreement of the participants who use them and are therefore limited to small, well-networked communities.

Today's financial system is based on a multitiered architecture of **explicit ledgers**.

Then who controls those ledgers?

# Ledgers




Source: On Distributed Communications Networks, Paul Baran, 1962.

# Ledgers

In a centralized system, a predefined set of agents is given an exclusive authority to manage the ledger. For example, the central banks keep ledgers of the assets of the commercial banks. The commercial banks in turn keep ledgers of their clients' assets.

In a decentralized system, every participant has a copy of the ledger.

Which arrangement is better? To answer this question, we consider the requirements of transaction execution.

# Transactional Requirements

There are three transactional requirements:

(1) **Transactional capacity**. This requirement ensures that transactions can be initiated and value units transferred.

(2) **Transactional legitimacy**. This requirement ensures that there is a control mechanism to guarantee that transactions may only be initiated by the rightful owner(s).

(3) **Transactional consensus**. This requirement ensures that there is a process which establishes an unambiguous distribution of ownership of all monetary units at all times.

# Transactional Requirements

For physical monetary units, these three requirements are automatically satisfied.

For virtual monetary units, a centralized ledger system can also satisfy these three requirements. However, the disadvantages of a centralized ledger system cannot be overlooked: monopoly rents, single point of failure, arbitrary confiscations...

How about a decentralized ledger system?

# I. Introduction: Bitcoin and Its predecessors

# Digital Currencies Before Bitcoin

Before the launch of Bitcoin, there were numerous attempts to create digital currencies that could serve as alternatives to fiat currency.

Three basic questions for users accepting digital money are:

- Can I trust that the money is authentic and not counterfeit?
- Can I trust that the digital money can only be spent once (known as the "double-spend" problem)?
- Can I be sure that no one else can claim this money belongs to them and not me?

# Digital Currencies Before Bitcoin

Questions for regulators accepting digital money are:

- How to enforce KYC (know your customer), AML (anti-money laundering) and CTF (counter-terrorism financing) regulations?
- Will it potentially destabilize traditional financial systems?
- How to conduct monetary policy in the digital currency era?
- Potential technological failures and cybersecurity risks.

# DigiCash

- https://www.chaum.com/ecash
- Founded by David Chaum in 1994 based on his paper published in 1984, DigiCash facilitates anonymous digital payments online.
- Cyberbucks
- Secure microchipped smart card
- Lack of merchants, DigiCash filed for bankruptcy in 1998.

# E-Gold

- https://en.wikipedia.org/wiki/E-gold
- Established in 1996, E-gold was backed by real units of precious metal.
- Micropayments: you can transact as small as one ten-thousandth of a gram of gold.
- E-Gold provides API to developers to build additional services on top of their platform.
- The US government shut down E-Gold.

# Hashcash

- http://www.hashcash.org
- Invented by Adam Back in 1997
- Introduced the idea of using proof-of-work to verify the validity of digital funds
- This system is proposed to reduce email spam

# B-Money

- http://www.weidai.com/bmoney.txt
- Introduced by Wei Dai in 1998
- Proposed the concept of nongovernmental money supply
- Advanced the idea of broadcasting transactions to a network
- Introduced the idea of using proof-of-work to create money
- B-Money is mainly a thought experiment

# Bit Gold

- https://nakamotoinstitute.org/bit-gold/
- Proposed in 2005 by Nick Szabo
- Bit Gold wants to issue digital gold like E-gold
- A trustless version of E-gold
- Bit Gold is largely a thought experiment

# Let us go back to 2008...

- Google Map, Baidu Map
- IM apps: MSN, QQ, Skype
- Amazon, Taobao
- Paypal, Alipay
- iPhone, Android Phone
- Financial Crisis

# Bitcoin Debut

In the Genesis block of bitcoin, Satoshi Nakamoto left a message,
*"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks."*

```
I've been working on a new electronic cash system that's fully
peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:
 Double-spending is prevented with a peer-to-peer network.
 No mint or other trusted parties.
 Participants can be anonymous.
 New coins are made from Hashcash style proof-of-work.
 The proof-of-work for new coin generation also powers the
    network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System
```


THE TIMES

Saturday January 3 2009 timesonline.co.uk No 69523 £1.50

Eat Out from £5

More than 900 great restaurants, including four Gordon Ramsay favourites from £15

Start collecting tokens today. Pullout inside

Israel prepares to send tanks and troops into Gaza

Israel allowed foreigners to flee the Gaza Strip as it prepared for a ground offensive. At least 430 Palestinians were killed in a week of airstrikes. News, page 3

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Francis Elliott Deputy Political Editor
Gary Duncan Economics Editor

99p

Michael Sheen Frost, Nixon and me

Working mums So that's how she does it

Detox in style The best spas on the planet

Travel

Salmon Rushdie I Won't Marry Again

Pages 22, 23

Giant Killing? Guide to the FA Cup Third Round

Sport

Source: https://www.bitcoin.com/satoshi-archive/emails/cryptography/1

# History of Bitcoin

Bitcoin was first described in 2008 with the publication of a paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System," written under the alias of Satoshi Nakamoto.

The Bitcoin network started in 2009 by Nakamoto, and since then the system has been revised by many other programmers.

Satoshi Nakamoto withdrew from the public in April 2011, leaving the responsibility of developing the code and network to a thriving group of volunteers. BitcoinCore.org, Bitcoin.org

# Why Bitcoin took off?

- Open source
  It is not proprietary, every one can check the code.
- Distribution
  Use decentralized nodes to maintain the record of transactions.
- Consensus
  Use Proof-of-Work to maintain the security of the bitcoin network.
- Right timing
  The technology is ready, people are ready.

# Bitcoin Overview

In this class, we use *bitcoin* to represent the unit of currency, and the system is called *Bitcoin*, with a capital *B*.

Bitcoin consists of:

- A decentralized peer-to-peer network (the Bitcoin protocol)
- A public transaction journal (the blockchain)
- A set of rules for independent transaction validation and currency issuance (consensus rules)
- A mechanism for reaching global decentralized consensus on the valid blockchain (proof-of-work algorithm)

# Bitcoin Wallet

**Bitcoin Wallet**: Bitcoin wallets are one of the most actively developed applications in the Bitcoin ecosystem.

(1) Bitcoin wallets can be categorized based on platforms:

- **Desktop wallet**: the first type of Bitcoin wallet. It runs on general-use operating systems, like Windows and macOS, which can be insecure and poorly configured.
- **Mobile wallet**: the most common type of Bitcoin wallet. To avoid downloading and storing large amounts of data, most mobile wallets retrieve information from remote servers, reducing your privacy by disclosing to third parties information about your Bitcoin addresses and balances.

# Bitcoin Wallet

(1) Bitcoin wallets can be categorized based on platforms:

- **Web wallet**: can be accessed through a web browser and store the user's wallet on a server owned by a third party. It is inadvisable to store large amounts of bitcoin on third-party systems.
- **Hardware signing devices**: devices that can store keys and sign transactions using special-purpose hardware and firmware. By handling all Bitcoin-related operations on the specialized hardware, these wallets are less vulnerable to many types of attacks.

# Bitcoin Wallet

(2) Bitcoin wallets can also be categorized based on the degree of autonomy:

- **Full node**: a full node wallet validates the entire history of Bitcoin transactions and it uses substantial computer resources. Full node wallet offers its users complete autonomy.
- **Lightweight client**: also known as a simplified-payment-verification (SPV) client. It only stores the user wallet locally and connects to a full node for receiving and sending transaction information. lightweight client partially validates the transactions it receives, and independently creates outgoing transactions.

# Bitcoin Wallet

(2) Bitcoin wallets can also be categorized based on the degree of autonomy:

- **Third-party API client**: interacts with Bitcoin through a third-party system of APIs rather than by connecting to the Bitcoin network directly. The wallet may be stored by the user or by third-party servers, but the client trusts the remote server to provide it with accurate information and protect its privacy. Third-party API client offers its users the least autonomy.

# How Bitcoin Works

Alice just set up her first Bitcoin wallet and she has bought some bitcoins from her friend Joe. Now Alice wants to make her first spending transaction: purchase one podcast episode from Bob.

Bob's e-commerce system will automatically create a QR code containing an invoice:

Figure 2: Invoice QR code

Source: Mastering Bitcoin - Programming the Open Blockchain, Andreas M. Antonopoulos , David A. Harding

# How Bitcoin Works

The invoice QR code encodes the following URI, defined in BIP21:

```
bitcoin:bc1qk2g6u8p4qm2s2lh3gts5cpt2mrv5skcuu7u3e4?amount=0.01577764&
label=Bob%27s%20Store&
message=Purchase%20at%20Bob%27s%20Store

Components of the URI

A Bitcoin address: "bc1qk2g6u8p4qm2s2lh3gts5cpt2mrv5skcuu7u3e4"
The payment amount: "0.01577764"
A label for the recipient address: "Bob's Store"
A description for the payment: "Purchase at Bob's Store"
```

# How Bitcoin Works

Around 10 minutes after the transaction is finalized, Bob can use a block explorer to see that this transaction is recorded in the Bitcoin blockchain.

Popular Bitcoin blockchain explorers:

- Blockstream Explorer
- Blockchain Explorer
- Mempool.Space
- BlockCypher Explorer

In the next sections, we will examine this transaction in more detail.

# Bitcoin Transactions

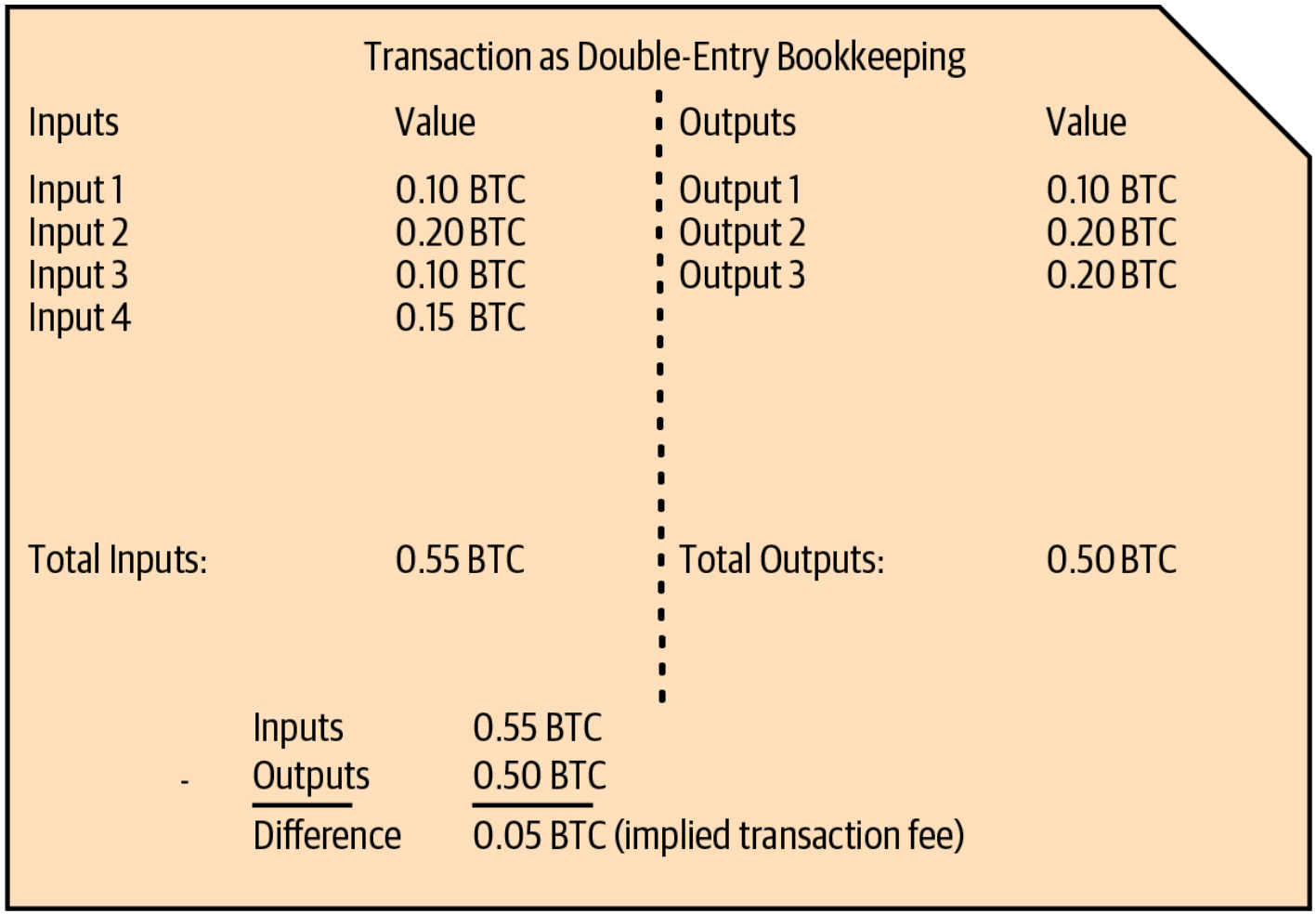



Figure 3: Transaction as double-entry bookkeeping
Source: Mastering Bitcoin - Programming the Open Blockchain, Andreas M. Antonopoulos , David A. Harding

# Transaction Chains

Alice's payment to Bob's Store uses a previous transaction (with Joe)'s output as its input. Tx1 sent 0.001 bitcoins (100,000 satoshis) to an output locked by Alice's key. In Tx2 Alice paid 75,000 satoshis for the podcast.

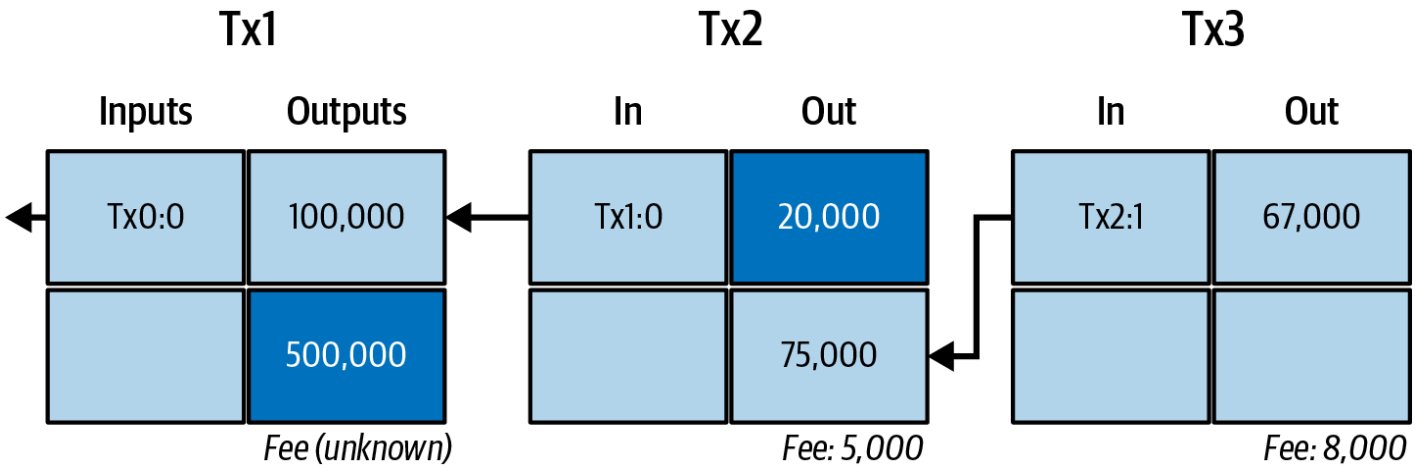



Figure 4: A chain of transactions

Source: Mastering Bitcoin - Programming the Open Blockchain, Andreas M. Antonopoulos , David A. Harding

# Transaction Propagation

Alice's wallet application sends the new transaction to any Bitcoin node.

After validating the transaction, the Bitcoin node(s) will forward it to all other nodes to which it is connected, a propagation technique known as **gossiping**.

Thus, the transaction rapidly propagates out across the peer-to-peer network, reaching a large percentage of the nodes within a few seconds.

# Mining

Alice's transaction is now propagated on the Bitcoin network.

However, this transaction does not become part of the blockchain until it is included in a block by a process called **mining** and that block has been validated by full nodes.

The mining mechanism serves as the counterfeit protection in the Bitcoin system.

Miners can receive bitcoin reward through the mining process (Coinbase reward + TX fee).

# Transaction Confirmation

After a candidate block that contains Alice's transaction is approved by all the nodes in the Bitcoin network, we can say this transaction is confirmed and it has got **one confirmation**.

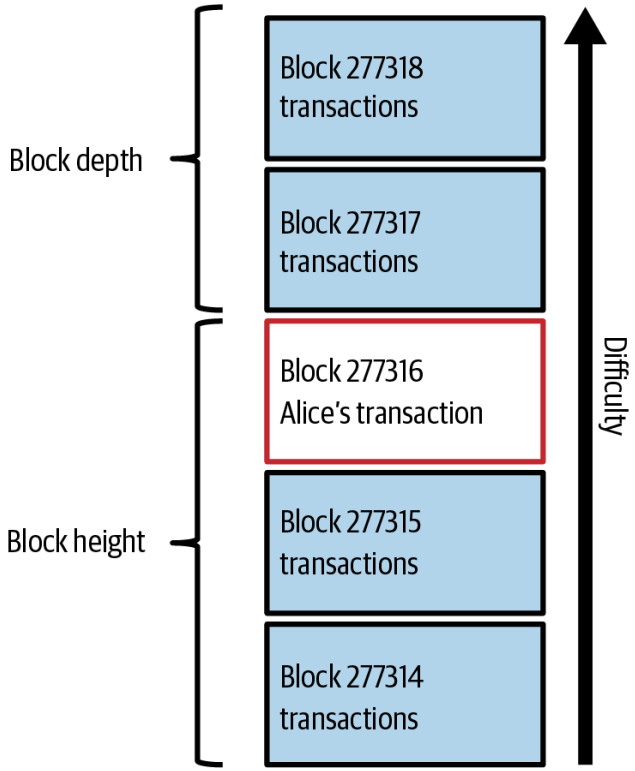



Figure 5: Alice's transaction included in a block
Source: Mastering Bitcoin - Programming the Open Blockchain, Andreas M. Antonopoulos , David A. Harding

# Bitcoin Concepts

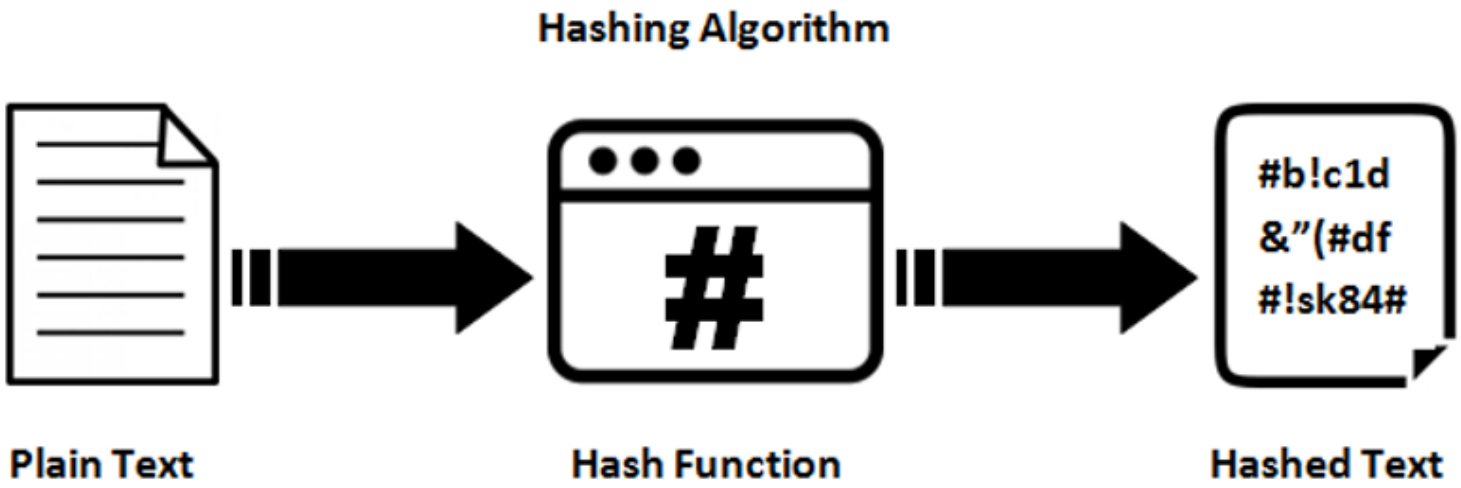
(1) **Double spending**
The risk that a unit of currency is spent more than one time.

(2) **Proof-of-work**
The solution to a mathematical problem. It is used as the consensus mechanism in bitcoin.

(3) **Nonces**
A random number used to meet the goal set by proof-of-work.

(4) **Hash function**
A hash function is any function that can be used to map data of arbitrary size to fixed-size values (called *hash*).

# Hash Function




Plain Text: arbitrary length
Hashed Text: certain length (for example, 32 bytes)
SHA-256: https://www.movable-type.co.uk/scripts/sha256.html

# Bitcoin Concepts

(5) **Block hash**
A unique identifier of a block.

(6) **Transaction hash**
A unique identifier of a transaction.

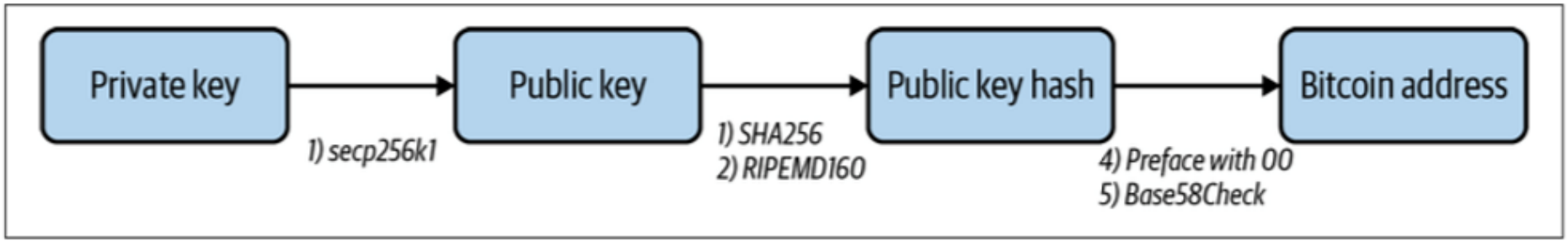
(7) **Coinbase transaction**
The first transaction in each block, and it is used to reward the miner who successfully minted/confirmed the block.

(8) **Block height number**
It measures the distance between the referred block and the first block.

(9) **UTXO**
Unspent Transaction Output

# Public-key cryptography

- The system includes a pair of keys: public key and private key
- The cryptography is widely used and has been proved to be reliable, e.g. end-to-end encryption
- Private key is used to sign a transaction
- Public key is used to generate the bitcoin address




Source: Mastering Blockchain, Lorne Lantz & Daniel Cawrey

# References


- Kocherlakota, Narayana R. "Money is memory." Journal of economic theory 81.2 (1998): 232-251.
- Menger, Karl. "On the origin of money." General Equilibrium Models of Monetary Economies. Academic Press, 1989. 67-82.