

# Blockchain in Cryptocurrency

Niko Tsutskiridze



# Agenda

01

**Blockchain Technology**

02

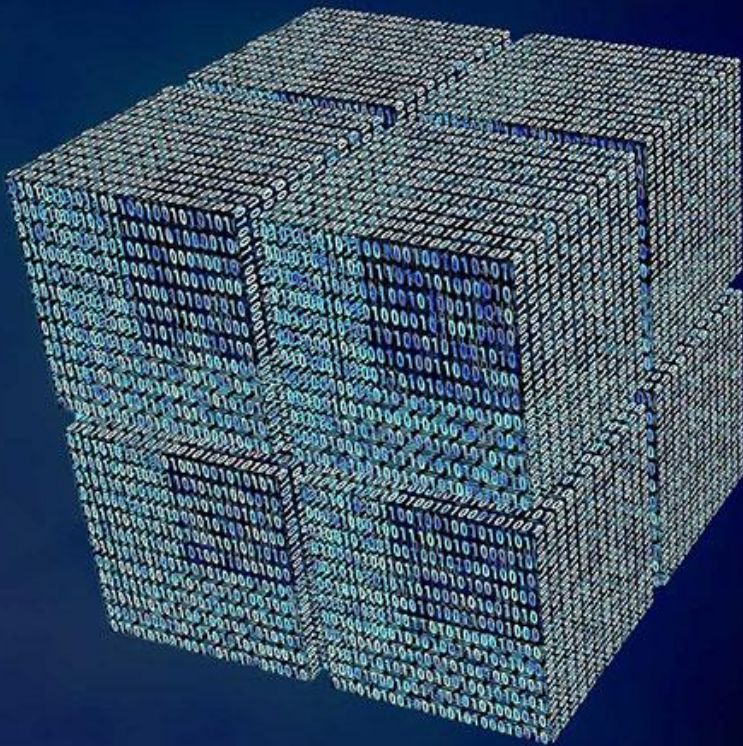
**Mining**

03

**Cryptocurrency**

04

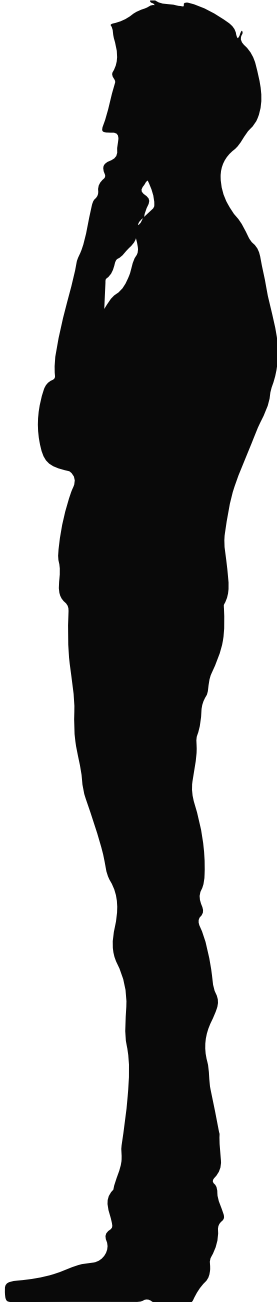
**Digital Money**



# The First Story

January 3, 2009

**Satoshi Nakamoto** activated the Bitcoin mainnet and obtained the first block containing 50 Bitcoins.



Who is Satoshi Nakamoto?  
- Who Knows?!

```

RAW HEX VERSION
BITCOIN GENESIS BLOCK

00000000 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000020 00 00 00 00 3B A3 ED FD 7A 7B 12 B2 7A C7 2C 3E ....;fiyz{.²zÇ,>
00000030 67 76 8F 61 7F C8 1B C3 88 8A 51 32 3A 9F B8 AA gv.a.È.Ã`ŠQ2:Ÿ,š
00000040 4B 1E 5E 4A 29 AB 5F 49 FF FF 00 1D 1D AC 2B 7C K.^J)«_Iÿÿ...~+|
00000050 01 01 00 00 00 01 00 00 00 00 00 00 00 00 00 .....
00000060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000070 00 00 00 00 00 00 FF FF FF FF 4D 04 FF FF 00 1D .....ÿÿÿÿM.ÿÿ..
00000080 01 04 45 54 68 65 20 54 69 6D 65 73 20 30 33 2F ..EThe Times 03/
00000090 4A 61 6E 2F 32 30 30 39 20 43 68 61 6E 63 65 6C Jan/2009 Chancel
000000A0 6C 6F 72 20 6F 6E 20 62 72 69 6E 6B 20 6F 66 20 lor on brink of
000000B0 73 65 63 6F 6E 64 20 62 61 69 6C 6F 75 74 20 66 second bailout f
000000C0 6F 72 20 62 61 6E 6B 73 FF FF FF FF 01 00 F2 05 or banksÿÿÿÿ..ð.
000000D0 2A 01 00 00 00 43 41 04 67 8A FD B0 FE 55 48 27 *....CA.gŠÿ°pUH'
000000E0 19 67 F1 A6 71 30 B7 10 5C D6 A8 28 E0 39 09 A6 .gñ;q0·.\Ö''(à9.¡
000000F0 79 62 E0 EA 1F 61 DE B6 49 F6 BC 3F 4C EF 38 C4 ybàè.ad†IÖ¿?Ll8Ä
00000100 F3 55 04 E5 1E C1 12 DE 5C 38 4D F7 BA 0B 8D 57 óU.â.Á.Þ\8M+ø..W
00000110 8A 4C 70 2B 6B F1 1D 5F AC 00 00 00 00 ŠLp+kñ._~....

```



[Home](#) > [Journal of Cryptology](#) > [Article](#)

[Published: January 1991](#)

## How to time-stamp a digital document

[Stuart Haber](#) & [W. Scott Stornetta](#)

[Journal of Cryptology](#) **3**, 99–111 (1991) | [Cite this article](#)

**24k** Accesses | **518** Citations | **745** Altmetric | [Metrics](#)

### Abstract

The prospect of a world in which all text, audio, picture, and video documents are in digital form on easily modifiable media raises the issue of how to certify when a document was created or last changed. The problem is to time-stamp the data, not the medium. We propose computationally practical procedures for digital time-stamping of such documents so that it is infeasible for a user either to back-date or to forward-date his document, even with the collusion of a time-stamping service. Our procedures maintain complete privacy of the documents themselves, and require no record-keeping by the time-stamping service.

<https://link.springer.com/article/10.1007/BF00196791>



# Blockchain technology

- Safety
- Decentralization
- Confidentiality

## Blockchain

Blockchain is a technology that enables the secure sharing of information.

Notes, lists, transactions etc.

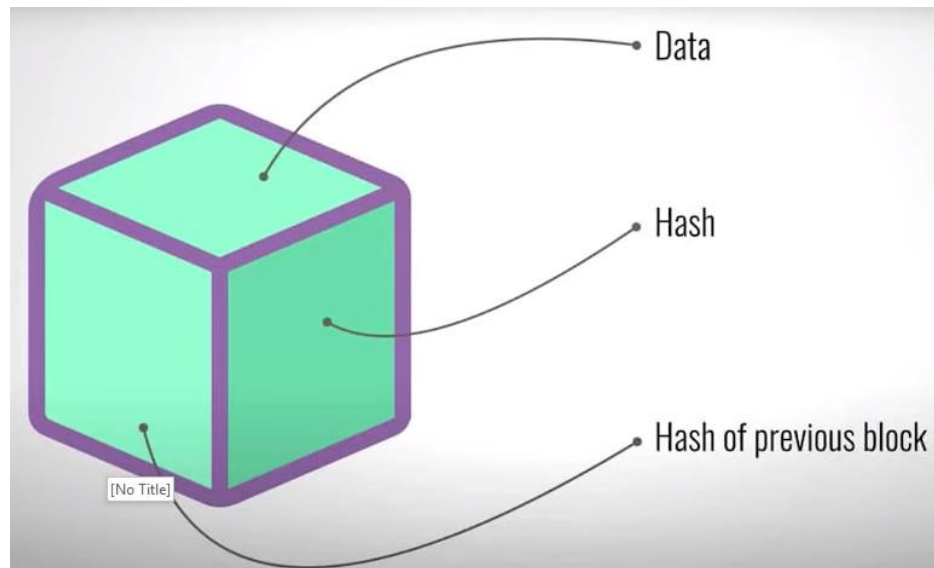
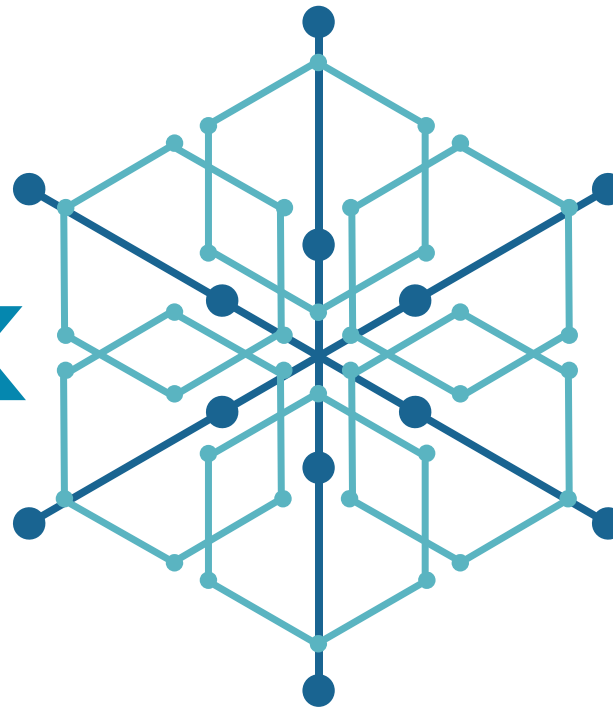
# BLOCK

**Data** - in the case of Bitcoin, a block contains data about transactions: the sender, the recipient, and the number of Bitcoins sent.

Each block in the blockchain includes some kind of **data** (depending on the type of blockchain), the **hash** of that block and the **hash of the previous block**.

# CHAIN

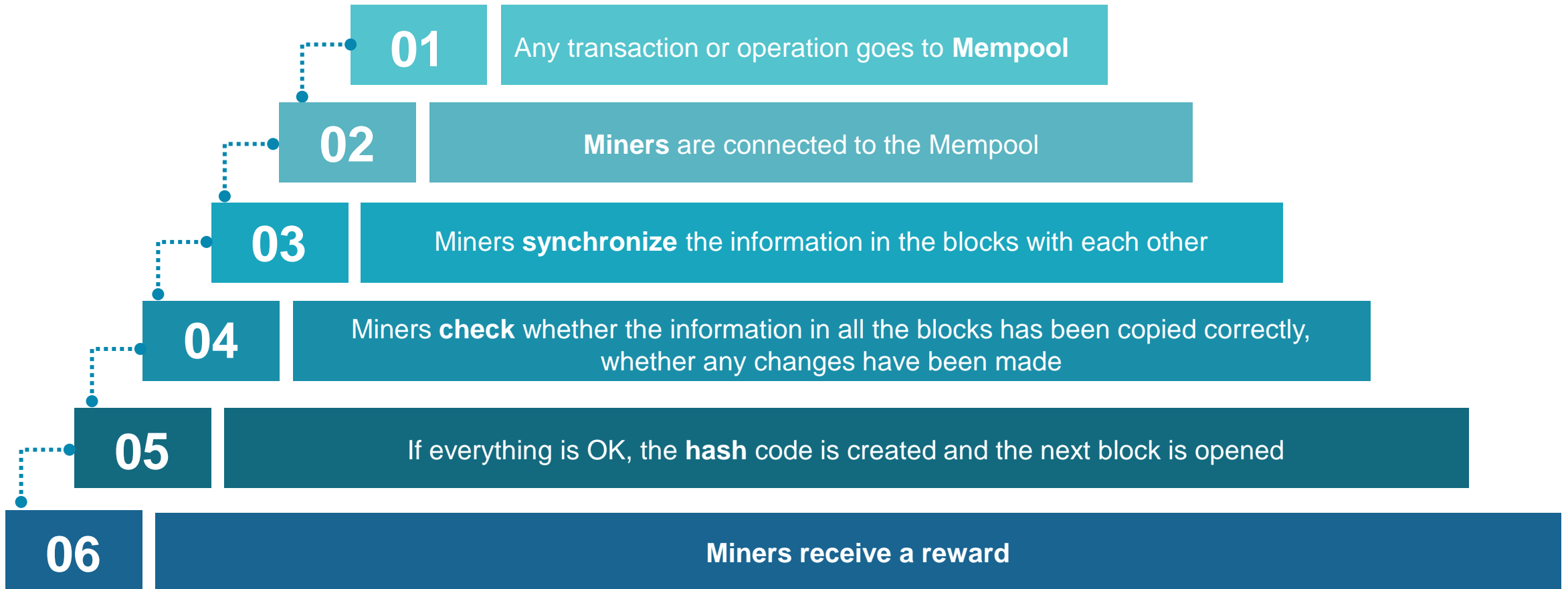
**Hash** - we can compare it to a fingerprint. It identifies the information in the block and it is unique.



# Safety – 50% + 1

Blockchain is served by **Mempool**

A **Mempool** is a blockchain node's waiting room for queued and pending transactions



# Mining

Bitcoin mining - the same as earning bitcoins Bitcoin works on the principle of a single-level network. Which means that each user owns a small fraction of Bitcoin

## Where does bitcoin come from?

- It is generated by solving a mathematical algorithm, in which the user receives a certain amount of Bitcoin. This ensures the creation of currency and the motivation to attract additional miners.

As more miners join the system, the Bitcoin server becomes more difficult to solve the algorithm.

Mining requires special software and appropriate hardware





# Decentralization / Confidentiality

## Decentralization

Bank - a **centralized** institution.

- The bank owns and manages your assets and stores your personal information
- Since all information is stored on "one server", it can become accessible to a hacker.

**In blockchain, decentralization** refers to the transfer of control and decision-making from a centralized entity (individual, organization, or group thereof) to a distributed network.

## Confidentiality

In the case of banks, you provide information to the banks during any transaction.

**In case of blockchain** you need **Public Kay** and **Private Kay**.

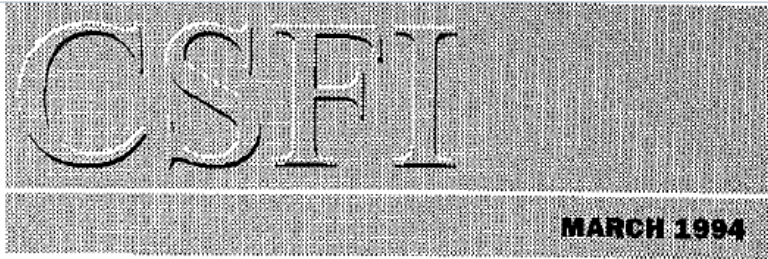
- **Public Kay** is your wallet address. The same bank account number with no information behind it.

- **Private Kay** - your private key with which you can access, unlock, restore your private wallet. P.S. Must be stored in a safe place. If you lose, you lose your money.

There are 2 ways to transfer money

- Personal
- With the intervention of a third person

# Cryptocurrencies



## The IBM dollar

By Edward de Bono

Republished with permission from  
[The Centre for the Study of Financial Innovation](http://www.csfi.org/)  
<http://www.csfi.org/>



The IBM Dollar

### Executive summary

The financial markets provide us with the means of investing in large companies and buying their products. They do not, however, enable us to invest in future production. Such an arrangement would bring advantages both to production companies and their customers, and it should be possible using the notion of "target currencies".

This paper proposes that large manufacturing corporations should create their own special currencies which would be exchangeable for, or "targeted" on, their products. IBM, for example, could sell "IBM dollars" which entitled the purchaser to buy a stated amount of computer equipment at a future date. The currency would be issued at a discount from its face value, the discount being determined by reference to interest rates, the perceived value of IBM products, and the level of market confidence in IBM's ability to remain competitive. At the redemption date the purchaser would exchange the currency, at face value, for equipment.

1994 - an article was published that changed many people's views on money.

The article was called: **The IBM dollar**, by Edward de Bono

His vision about money was that technological transformations in computer technology and cryptography would make money production so cheap that private companies would create their own digital currency instead of releasing their own securities. This, in turn, calls into question the activities of central banks.

# Cryptocurrencies



[No Title]

- January 3, 2009 - Satoshi Nakamoto activated the Bitcoin mainnet and earned the first block containing 50 bitcoins.
- April 23, 2011 - Satoshi's last message was published:

From: Satoshi Nakamoto <satoshin@gmx.com>

Date: Sat, Apr 23, 2011 at 3:40 PM

To: Mike Hearn <mike@plan99.net>

> I had a few other things on my mind (as always). One is, are you planning on rejoining the community at some point (eg for code reviews), or is your plan to permanently step back from the limelight?

I've moved on to other things. It's in good hands with Gavin and everyone.

# Cryptocurrencies



- When Bitcoin was first invented, central bankers loved this new innovation
- But national governments were wary of it because its anonymity allowed illegal activity to take place
- In 2014, central banks, such as China's central bank, began actively fighting against Bitcoin. Chinese banks were banned from using them
- Like ordinary currencies, cryptocurrencies do not have inherent value, but unlike money, cryptocurrencies do not have corresponding obligations, for example, they do not obey central banks, the main purpose of which is to maintain its value
- The value of cryptocurrency is determined by the desire of the parties involved in its transaction
- Nevertheless, cryptocurrencies have already appeared on the market as a means of payment.

For example, Tesla uses dogecoin as a payment method.



# Cryptocurrencies

cryptocurrency by a ticket - Google x Flight Search | Alternative Airlines x

alternativeairlines.com/flights/TBS-GVA?outbound=2023-09-01&return=2023-10-05&adults=1&children=0&infants=0&class=Y&currency=GEL&lp...

Where from? Tbilisi (TBS) Where to? Geneva (GVA) Departure date 01/09/2023 Return date 05/10/2023 Passengers 1 Adult, Economy Search Flights

Quickest  
 Lowest Emissions

Currency: GEL

Stops:  
 Up to 1 Stop 1,294.73 ₾  
 Up to 2 Stops 1,642.12 ₾

Times:

7228.51049 DOGE ⓘ  
1,345.58 ₾ total Recommended

Tbilisi → Geneva Fri 1 Sep

<input type="checkbox"/>	TURKISH AIRLINES	Fri 1 Sep 05:50	Tbilisi	TBS	10h 20m	1 stop	GVA	Fri 1 Sep 14:10	Details ▾
--------------------------	------------------	--------------------	---------	-----	---------	--------	-----	--------------------	-----------

Geneva → Tbilisi Thu 5 Oct

<input type="checkbox"/>	TURKISH AIRLINES	Thu 5 Oct 15:00	Geneva	GVA	10h 15m	1 stop	TBS	Fri 6 Oct 03:15	Details ▾
<input type="checkbox"/>	TURKISH AIRLINES	Thu 5 Oct 19:20	Geneva	GVA	12h 35m	1 stop	TBS	Fri 6 Oct 09:55	Details ▾

This website uses cookies. [More Info](#) OK

Windows Search | ENG | 18:05 23.05.2023

# Digital money



- However, in the era of finance, a new digital era has begun
- Even during the pandemic, the People's Bank of China has announced that it is starting to test its own digital currency
- Employees of government organizations in 4 test cities of China received their salaries in digital yuan.
- However, it is completely different from Bitcoin for example. It does not apply to digital yuan Blockchain technology and it is fully regulated by the central bank.

# Today's Cryptocurrency Prices by Market Cap

The global crypto market cap is **\$1.13T**, a **▼ 0.54%** decrease over the last day. [Read Less](#)

The total crypto market volume over the last 24 hours is **\$46.65B**, which makes a **▲ 51.81%** increase. The total volume in DeFi is currently **\$3.32B**, 7.11% of the total crypto market 24-hour volume. The volume of all stable coins is now **\$42.11B**, which is **90.26%** of the total crypto market 24-hour volume.

Bitcoin's dominance is currently **46.94%**, a decrease of **▼ 0.02%** over the day.

CoinMarketCap reports that **there are approximately 22,932 cryptocurrencies**, with a total market capitalization of \$1.1 trillion. That's quite a crowd considering that Bitcoin only launched in 2009.

# Cryptocurrencies

# ▲	Name	Price	1h %	24h %	7d %	Market Cap ⓘ	Volume(24h) ⓘ	Circulating Supply ⓘ	Last 7 Days
☆ 1	Bitcoin BTC <a href="#">Buy</a>	\$27,409.91	▼ 0.22%	▼ 0.66%	▼ 5.81%	\$530,933,385,076	\$21,041,029,975 767,118 BTC	19,370,125 BTC	
☆ 2	Ethereum ETH <a href="#">Buy</a>	\$1,819.32	▼ 0.60%	▼ 1.08%	▼ 4.35%	\$218,881,945,177	\$10,471,090,084 5,751,242 ETH	120,309,683 ETH	
☆ 3	Tether USDT	\$1.00	▲ 0.02%	▲ 0.03%	▲ 0.03%	\$82,674,155,940	\$32,367,995,037 32,346,747,159 USDT	82,612,464,847 USDT	
☆ 4	BNB BNB <a href="#">Buy</a>	\$311.34	▲ 0.03%	▼ 0.12%	▼ 4.53%	\$48,522,965,200	\$554,050,134 1,779,581 BNB	155,850,525 BNB	
☆ 5	USD Coin USDC	\$1.00	▼ 0.03%	▼ 0.00%	▲ 0.01%	\$30,132,462,527	\$4,656,191,761 4,655,466,188 USDC	30,129,862,186 USDC	
☆ 6	XRP XRP	\$0.4228	▼ 0.92%	▼ 0.47%	▼ 8.30%	\$21,917,569,460	\$1,014,427,363 2,397,864,702 XRP	51,837,820,505 XRP	



# “Funny” Stories



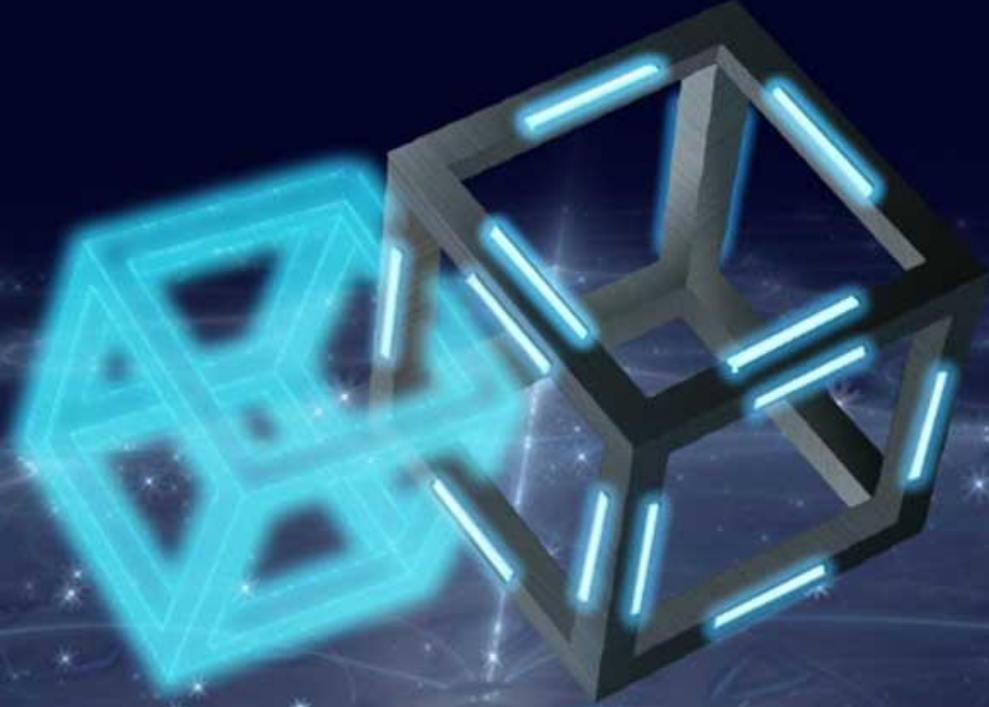
**BITCOIN**

On May 22, 2010, the software developer under the nickname Laszlo bought two of the most expensive pizzas ever sold. He paid 10,000 BTC for 2 pizzas (\$270,000,000 in today's value)

American journalist Mark Frauenfelder lost access to the wallet that stored 7 bitcoins purchased at the beginning of 2016 for three thousand dollars (today's value is \$189,000).

In general, 20% of existing bitcoins (\$106,186,677,015) are stored in wallets whose owners have lost access to them.





THANK YOU